NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 21 | Issue 3 Article 6

3-1-2020

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

Madeline A. Labovitz

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 21, ISSUE 3: MARCH 2020

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

Madeline A Labovitz*

In the past two decades, the United States has increased the production and use of natural gas to fuel every day American life. This increase has resulted in the construction of millions of miles of natural gas pipelines. While this development has produced a number of benefits, natural gas pipelines have introduced the threat of cyberattacks on natural gas infrastructure. This substantial threat is currently managed by voluntary guidelines promulgated by the Transportation Security Administration ("TSA"). While the private industry is satisfied to maintain the status quo and leave these threats essentially self-regulated, voluntary guidelines are not sufficient to defend against the cybersecurity threats posed to natural gas pipelines. This Recent Development proposes that cybersecurity standards should become mandatory and that the Department of Energy, not TSA, is the proper agency to promulgate mandatory cybersecurity regulations.

* J.D. Candidate, University of North Carolina School of Law, 2021. This article would not be possible without the invaluable guidance from Professor Jonas Monast and Professor Donald Hornstein. Thank you to my student note editor, executive editors, and the entire N.C. JOLT team for their support throughout the process.

I. INTRODUCTION

Today, the U.S. is the world's largest natural gas producer.[1] By 2020, the U.S. is projected to be the world's third largest exporter of liquified natural gas.[2] Natural gas is a volatile and dangerous product generally transported by pipelines that have largely computerized

[1] *See* SARAH LADISLAW ET AL., U.S. NATURAL GAS IN THE GLOBAL ECONOMY 1 (2017); Alex Dewar et al., *Preparing for an Abundance of US Natural Gas*, BOS. CONSULTING GROUP (Apr. 15, 2019), https://www.bcg.com/publications/2019/united-states-us-abundance-natural-gas.aspx [https://perma.cc/QZ77-CPRG].
[2] Dewar et al., *supra* note 1.

operations.[3] While computerization has allowed the millions of miles of American pipelines to operate efficiently, the technology has rendered natural gas pipelines vulnerable to sophisticated cyberattacks from adversaries.[4]

To combat this threat, cybersecurity of natural gas pipelines has been left exclusively to the Transportation Security Administration ("TSA").[5] TSA, to the satisfaction of the private industry, has only released voluntary guidelines leaving natural gas pipelines essentially self-regulated.[6] However, there has been push back by policy makers and agencies to vest different agencies with the ability to exact stronger natural gas pipeline cybersecurity regulations.[7]

In Part II, this article will discuss the background of natural gas in the U.S. and the general risks posed by natural gas production and transportation. As the interdependency between natural gas pipelines and the electric grid is steadily increasing, Part III will discuss the cybersecurity threats energy infrastructure faces in general. Part IV will specifically describe the cybersecurity threats posed to natural gas pipelines. Part V will detail the regulatory scheme, or lack thereof, in place to address and combat natural gas pipeline cybersecurity threats. Part VI will argue that the voluntary guidelines that currently instruct natural gas pipeline cybersecurity should be mandatory. Finally, Part VII will advocate that as the

---

[3] *See How Does the Natural Gas Delivery System Work?*, AMERICAN GAS ASS'N, https://www.aga.org/natural-gas/delivery/how-does-the-natural-gas-delivery-system-work-/ [https://perma.cc/VR6F-9FT9].

[4] *See Cybersecurity Threats Impacting the Nation: Hearing Before the Subcomm. on Oversight, Investigations, and Mgmt., Comm. on Homeland Sec.*, 112th Cong. 3 (statement of Gregory C. Wilshusen, Director of Information Security Issues), https://www.gao.gov/assets/600/590367.pdf.

[5] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-19-48, CRITICAL INFRASTRUCTURE PROTECTION: ACTIONS NEEDED TO ADDRESS SIGNIFICANT WEAKNESSES IN TSA'S PIPELINE SECURITY PROGRAM MANAGEMENT 1 (2018).

[6] TRANSPORTATION SECURITY ADMIN.: PIPELINE SECURITY GUIDELINES 1 (2018).

[7] *See* Rebecca Kern, *Looming Cybersecurity Battle: Who Protects U.S. Pipelines?*, BLOOMBERG ENV'T (June 22, 2018), https://news.bloomberg environment.com/environment-and-energy/looming-cybersecurity-battle-who-protects-us-pipelines-corrected [https://perma.cc/4Z99-VR98]; Blake Sobczak, *Battle lines form over pipeline cyberthreat*, E&E NEWS (July 25, 2019), https://www.eenews.net/stories/1060784805 [https://perma.cc/VW7F-P3WF].

guidelines become mandatory regulations, the Department of Energy ("DOE"), not TSA, should be the agency to promulgate natural gas pipeline cybersecurity regulations.

II. BACKGROUND OF NATURAL GAS IN THE UNITED STATES

Natural gas use is not confined to electricity generation; it is a versatile and multi-use product.[8] Natural gas has become an essential staple for most Americans.[9] Not only does natural gas heat one half of U.S. residents' homes and is used to cook their food, but natural gas is used for fuel, and for backup generators.[10] Further, as coal becomes obsolete, natural gas has become its replacement.[11]

Natural gas' prominence in the U.S. has grown considerably in recent decades to account for 31% of U.S. primary energy consumption today.[12] In the U.S., 34.1% of natural gas is used for fuel, 31.3% is used for industrial purposes, and 20.7% is used for cooking and heating.[13] Least substantially, 13.8% of natural gas is used for commercial purposes and 0.1% is used for vehicle fuel.[14]

Though natural gas plays such a significant role in American life, as recently as 2005, the U.S. was highly dependent on foreign

---

[8] Hobart M. King, *Uses of Natural Gas*, GEOLOGY.COM, https://geology.com/articles/natural-gas-uses/ (last visited Nov. 30, 2019) [https://perma.cc/R8KD-TBBF].

[9] *See id*.

[10] *Id*.; *History of the U.S. Natural Gas Industry,* DIRECT ENERGY, https://www.directenergy.com/learning-center/energy-choice/history-of-natural-gas-industry (last visited Nov. 30, 2019) [https://perma.cc/VP2Z-TUWU].

[11] *History of the U.S. Natural Gas Industry, supra* note 10.

[12] *U.S. Energy Facts Explained*, U.S. ENERGY INFO. ADMIN. (Aug. 28, 2019), https://www.eia.gov/energyexplained/us-energy-facts/ [https://perma.cc/D9QG-CUCJ]; *Glossary of Statistical Term: Primary Energy Consumptions*, ORG. FOR ECON. CO-OPERATION AND DEV., https://stats.oecd.org/glossary/detail.asp?ID=2112 (last visited Nov. 30, 2019) [https://perma.cc/B52H-EGXE]. "Primary energy consumption refers to the direct use at the source, or supply to users without transformation, of crude energy, that is, energy that has not been subjected to any conversion or transformation process." *Id.* Natural gas accounts for the second largest percentage of U.S. primary energy consumption. Petroleum makes up the largest percentage accounting for 36% of U.S. primary energy consumption. *Id.*

[13] King, *supra* note 8.

[14] *Id*.

imports of natural gas to meet demand.[15] This dependence led to historically high natural gas prices and predictions that the U.S. would experience a natural gas crisis in 2005.[16] However, the high prices, increasing demand, and continued reliance on foreign imports pushed the U.S. industry towards innovation. In the early 2000s, hydraulic fracturing was combined with horizontal drilling to enable, for the first time, oil and gas production from U.S. shale formations.[17]

Instead of the predicted natural gas crisis, in 2005, the new techniques led the U.S. to a natural gas boom and domestic production outpaced domestic need in 2015.[18] The increase in production, caused natural gas prices to plummet, decreasing from $13.42 per million BTUs in 2005 to $2.65 per million BTUs by the end of 2019.[19] The decreasing cost and increasing demand for natural gas, specifically in 2009, resulted in the construction of new natural gas pipelines.[20] Today, the U.S. contains nearly 3 million miles of pipelines used to deliver the approximately 30 trillion cubic feet of natural gas produced in the U.S.[21]

---

[15] *Natural Gas Explained: Use of Natural Gas*, U.S. ENERGY INFO. ADMIN. (July 10, 2019), https://www.eia.gov/energyexplained/natural-gas/use-of-natural-gas.php [https://perma.cc/7A8T-TC8C]; *see* LADISLAW ET AL., *supra* note 1.

[16] *See* LADISLAW ET AL., *supra* note 1.

[17] *Id*.; Robert Rapier, *How the Shale Boom Turned the World Upside Down*, FORBES (Apr. 21, 2017), https://www.forbes.com/sites/rrapier/2017/04/21/how-the-shale-boom-turned-the-world-upside-down/#7ef8bfa777d2 [https://perma.cc/9GPE-923C]. Hydraulic fracturing is technique that has been around since the 1940s that pumps water and a variety of chemicals down an oil or gas well to fracture reservoir rock and release natural gas. *Id*.

[18] *See* LADISLAW ET AL., *supra* note 1; Rapier, *supra* note 17.

[19] *Natural Gas Explained: Natural Gas Pipelines,* U.S. ENERGY INFO. ADMIN. (Dec. 5, 2019), https://www.eia.gov/energyexplained/natural-gas/natural-gas-pipelines.php [https://perma.cc/F6NP-ZGF6]; *Natural Gas: Henry Hub Natural Gas Spot Price*, U.S. ENERGY INFO. ADMIN., https://www.eia.gov/dnav/ng/hist/rngwhhdM.htm (last visited Nov. 30, 2019) [https://perma.cc/S25G-VBUN]. A "BTU" is a British Thermal Unit.

[20] *Natural Gas Explained: Natural Gas Pipelines, supra* note 19.

[21] *Id.*; *Natural Gas Explained: Where Our Natural Gas Comes From*, U.S. ENERGY INFO. ADMIN. (Nov. 13, 2019), https://www.eia.gov/energyexplained/natural-gas/where-our-natural-gas-comes-from.php [https://perma.cc/U72A-LMMM]; James Chen, *Trillion Cubic Feet (Tcf),* INVESTOPEDIA (Jan. 6, 2020), https://www.investopedia.com/terms/t/trillion-cubic-feet.asp

While natural gas plays a critical role in U.S. life and economy, there are some inherent dangers associated with natural gas use and production that amplify the danger of cybersecurity threats. For example, poorly maintained equipment can result in carbon monoxide poisoning.[22] Natural gas pipelines can also leak, leading to explosions.[23] Moreover, the computerization of natural gas pipelines has also led to unintentional damage as "software upgrades and defective equipment" can "inadvertently disrupt systems" and cause damage.[24]

Even absent a cybersecurity threat from an adversary, natural gas accidents in the U.S. have resulted in widespread service disruption, serious destruction and even death. For example, a natural gas pipeline exploded in San Francisco in 2019 when a construction company accidentally cut into the natural gas main.[25] The explosion, described as shooting a "tower of flames into the sky," seriously damaged a number of buildings.[26] Also in 2019, a natural gas pipeline in Durham, North Carolina caused an explosion

---

[https://perma.cc/AC7F-RNXS]. Natural gas increased to 30 Tcf from 19.18 Tcf of natural gas produced at the start of 2000. "Trillion cubic feet," or Tcf, is the unit used by the oil and gas industry to measure natural gas. The measurement can be difficult to quantify, and it is most commonly equated to one quadrillion of a British thermal unit, which represents the amount of heat "required to raise the temperature of a single pound of water by one-degree Fahrenheit at sea level." *Id.*

[22] *Natural Gas Safety*, OHIO PUBLIC UTILITIES COMM'N, https://www.puco.ohio.gov/be-informed/consumer-topics/natural-gas-safety/ (last visited Nov. 30, 2019) [https://perma.cc/5WK6-6MJS].

[23] *Id*.

[24] *Cybersecurity Threats Impacting the Nation: Hearing Before the Subcomm. on Oversight, Investigations, and Mgmt., Comm. on Homeland Sec.*, *supra* note 4.

[25] Dan Noyes, *What We Know About Gas Explosion in San Francisco*, ABC 7 NEWS (Feb. 7, 2019), https://abc7news.com/what-we-know-about-gas-explosion-in-san-francisco/5125028/ [https://perma.cc/FT3X-MYY4].

[26] Janie Har, *San Francisco Gas Explosion Shoots Fire that Burns 5 Buildings*, USA TODAY (Feb. 6, 2019), https://www.usatoday.com/story/news/2019/02/06/san-francisco-gas-line-explosion-buildings-fire/2796109002/ [https://perma.cc/GD7Q-5FFL].

when a "a gas service line was struck during a horizontal boring operation."[27] The explosion killed two people.[28]

The severe consequences a natural gas pipeline attack could have on life, property, the economy, and the environment combined with the volatility of the product makes pipelines highly attractive targets for those with malicious intent.[29] Adversaries can capitalize on the devastation natural gas naturally causes to threaten critical infrastructure and human life through a cyberattack on the pipelines that transport natural gas.[30] The technology used to operate and control natural gas pipelines serves as an entrance to those that seek to cause serious harm.

III. CYBER THREATS TO ENERGY INFRASTRUCTURE

According to the North American Electric Reliability Corporation's president and CEO, "the threat of [a] cyberattack is at an all-time high."[31] The Department of Homeland Security ("DHS") has similarly reported that over the past several years, the energy sector has "incurred more cybersecurity incidents than any other sector."[32] Moreover, DOE reported that the "frequency, scale, and sophistication of cyber threats have increased, and attacks have become easier to launch."[33] As natural gas pipelines have increasingly relied on computerized systems, adversaries may wish

---

[27] Josh Chaplin, *Durham Fire Department Releases Findings in Report on Deadly Downton Gas Explosion*, ABC EYEWITNESS NEWS 11 (Aug. 10, 2019), https://abc11.com/durham-fire-dept-releases-findings-in-report-on-deadly-gas-explosion/5456021/ [https://perma.cc/M7X4-3E9F].
[28] *Id*.
[29] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 5.
[30] *See* PIPELINE SECURITY: HOMELAND SECURITY ISSUES IN THE 116TH CONGRESS 1 (2019); *Physical Security*, INTERSTATE NATURAL GAS ASS'N OF AMERICA, https://www.ingaa.org/Pipelines101/Security/26508.aspx (last visited Nov. 30, 2019) [https://perma.cc/XTF3-5K2L].
[31] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 5.
[32] 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, 581 (2017).
[33] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 5, at 11–12.

to utilize pipelines to launch attacks with devastating consequences.[34]

While the U.S. has not yet experienced a cyberattack that resulted in death or a catastrophic disruption in the flow of oil or gas, cyberattacks on natural gas pipelines can result in significant physical damage such as "explosions, spills, or fires, which will easily threaten human life, property and the environment."[35] Cyberattacks can also lead to electricity production outages.[36] Foreign cyberattacks on energy infrastructure show how serious energy cyberattacks can be.

As the U.S. increases reliance on natural gas, the impact of a cyberattack on critical energy infrastructure is exacerbated.[37] The interdependency between natural gas pipelines and the electric grid has steadily increased. As a result, it is important to understand the threats to America's electric grid to recognize the risks natural gas pipelines face.

A. Ukraine's Electric Grid Cyberattack

In a display of the effectiveness of an energy infrastructure cyberattack, Ukrainian power companies experienced unscheduled power outages, affecting 225,000 local customers in December

---

[34] *Physical Security*, *supra* note 30; *see* HOMELAND SECURITY ISSUES IN THE 116TH CONGRESS, *supra* note 30; *see* Hillary Hellmann, Comment, *Acknowledging the Threat: Securing United States Pipeline SCADA Systems*, 36 ENERGY L.J. 157, 159 (2015). Liquid and gas transmission pipelines utilize SCADA technology to "control thousands of miles of pipelines from one central location. Human controllers can input commands to remotely operate pipeline control equipment" to control such components as pressure, temperature, and rate of oil or gas flow. *Id*.

[35] 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/S8MK-RT7G].

[36] *Id*.

[37] Elisabeth Buchwald, *The Use of Natural Gas Exposes U.S. to Cyber Attacks, FERC Chairman Says*, MARKET WATCH (Feb. 19, 2019), https://www.marketwatch.com/story/increased-use-of-natural-gas-exposes-us-to-cyber-attacks-ferc-chairman-says-2019-02-14 [https://perma.cc/8VPL-4QEV].

2015.[38] The power outages were determined to be the result of an external cyberattack.[39] DHS released a formal report detailing the attack, which stated that the attackers remotely targeted three regional electric power distribution companies and by "leveraging legitimate credentials obtained via unknown means, remotely operated breakers to disconnect power" and "wiped some systems by executing the KillDisk malware at the conclusion of the cyberattack."[40]

The cyber-attackers utilized known methods of cyber intrusions and techniques that had not before been used in a cyberattack.[41] The initial intrusion came from spear-phising, whereby an attack originates in a business system and "migrate[s] to operations systems."[42] Attackers sent emails with malicious Microsoft Office documents that contained the malware used to gain access to the electricity company's networks.[43] This enabled the attackers to the steal credentials necessary to access the company's network allowing the attackers to issue commands remotely in order to schedule service outages.[44] The attackers were also able to access telephone systems in order to generate an overload of calls to the energy company denying access to customers attempting to report outages.[45]

---

[38] ROBERT M. LEE ET AL., ANALYSIS OF THE CYBER ATTACK ON THE UKRAINIAN POWER GRID v (Electricity Information Sharing and Analysis Center 2016); *ICS Alert* (IR-ALERT-H-16-056-01) *Cyber-Attack Against Ukrainian Critical Infrastructure*, U.S. DEP'T OF HOMELAND SEC. (Aug. 23, 2018), https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01 [hereinafter *ICS Alert*] [https://perma.cc/6GDA-7GAC].

[39] *ICS Alert*, *supra* note 38.

[40] NCCIS/ICS-CERT INCIDENT ALERT, U.S. DEP'T OF HOMELAND SEC. (Mar. 7, 2016).

[41] *Id*.

[42] *Id*.; U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 5, at 13. Spear-phishing is sending a recipient official-looking emails that contain malware (harmful software programs) that will insert into a computer system and allow the sender to gain access to business information and confidential data. *Id.*

[43] NCCIS/ICS-CERT INCIDENT ALERT, *supra* note 40; LEE ET AL., *supra* note 38, at 1.

[44] *See* LEE ET AL., *supra* note 38, at 2.

[45] *See id*.

The Electricity Information Sharing and Analysis Center noted that the attacker's strongest capability was not the complexity of their cyberattack on Ukraine, but rather the attacker's ability to "perform long-term [surveillance] operations required to learn the environment and execute a highly synchronized, multistage, multisite attack."[46] The Ukrainian cyberattack took place immediately after "a political revolution in Kiev, the annexation of Crimea, and amid military clashes in the eastern Donetsk and Luhansk regions."[47] The U.S. government and cybersecurity firms attributed the Ukraine cyberattack to Russia as an act of cyber warfare.[48] While the Ukraine cyberattack was on the electric grid generally, it demonstrated "one nation's ability to disrupt another by shutting down operations and damaging physical equipment."[49]

The techniques demonstrated by Russia are transferable to natural gas pipelines. In fact, a Russian group, Black Ghost Knifefish," has targeted U.S. natural gas and highlights the growing concern of cyber warfare on energy infrastructure.[50]

B. Energy Infrastructure Cyberattacks Have Morphed into Cyber Warfare

Today, nations can "cause warlike damage to their enemy's vital infrastructure without launching a military strike."[51] In Ukraine, Russian intrusion into their electric grid resulted in power outages

---

[46] *See id*.
[47] Donghui Park et al., *Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks*, U. OF WASH. (Oct. 11, 2017), https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/ [https://perma.cc/5SFW-Q48Z].
[48] *Id*.
[49] Jean-Marc Ollagnier, *Cyberattacks are Becoming a Greater Challenge for the Energy Industry*, FORBES (Oct. 1, 2018), https://www.forbes.com/sites/jeanmarcollagnier/2018/10/01/the-next-cyberattack-staying-ahead-of-hackers-is-becoming-a-greater-challenge/#400a63bf4f0f [https://perma.cc/RZQ9-PHY6].
[50] *Id*.
[51] Beatrice Christofaro, *Cyberattacks are the Newest Frontier of War and Can Strike Harder than a Natural Disaster. Here's Why the US Could Struggle to Cope if it Got Hit*, BUS. INSIDER (May 23, 2019), https://www.businessinsider.com/cyber-attack-us-struggle-taken-offline-power-grid-2019-4 [https://perma.cc/98YH-5AC5].

for a quarter of a million people.[52] A shut down of the electric grid does not just result in darkness. Rather, phones and the internet do not work, transportation idles because fuel is inaccessible and charging stations are inoperable.[53] The same rings true for banks, ATMs, heating and air conditioning, which would not work.[54] Hospitals and emergency services would similarly not be available.[55]

While nearly everyone in the U.S. has experienced an electric outage from accidents or storms, the potential blackout that could come from an energy infrastructure cyberattack is unprecedented. Unlike a cyberattack, when a major natural disaster, like a hurricane, knocks out power, the U.S. can be reasonably certain when the hurricane will end. Further, hurricanes do not "return to strike a second or third time" and do not "replicate themselves in other parts of the country."[56] Connecticut's chief cybersecurity risk officer, Arthur House, predicted that within two weeks of a cyberattack caused power outage, the U.S. "might exhaust reserve fuel to generate utility services," "[p]ublic order would be strained," and "[t]he hit on commerce could be devastating."[57]

The Pentagon's Defense Advanced Research Projects Agency ("DARPA") is conducting projects to determine U.S. capabilities to recover from a cyberattack that caused power outages like that in Ukraine.[58] On the restrictive and secretive Plum Island, normally used to conduct research on infectious diseases, DARPA ran a program that simulated power grid deactivation that could ensue

---

[52] LEE ET AL., *supra* note 38, at iv.
[53] John E. Shkor & Timothy Connors, *Escalation of Cyber Warfare Puts US Electric Grid in Crosshairs*, REAL CLEAR POL'Y (Aug. 6, 2019), https://www.realclearpolicy.com/articles/2019/08/06/escalation_of_cyber_warfare_puts_us_electric_grid_in_crosshairs_111252.html [https://perma.cc/28LG-WF6C].
[54] *Id*.
[55] *Id*.
[56] Arthur H. House, *We'd be Crippled by a Cyberattack on our Utilities*, WASH. POST (Oct. 14, 2018), https://www.washingtonpost.com/opinions/wed-be-crippled-by-a-cyberattack-on-our-utilities/2018/10/14/206b0dc6-cca8-11e8-a360-85875bac0b1f_story.html [https://perma.cc/HM8W-MSV9].
[57] *Id*.
[58] Christofaro, *supra* note 51.

from an energy infrastructure cyberattack.[59] DARPA's program director, Walter Weiss, described the process of bringing the grid back from deactivation as "painstaking" and "slow."[60]

The federal government has taken steps to increase U.S. energy infrastructure cybersecurity. Executive Order 13800 called for an assessment of the detrimental effects that a prolonged power outage from a cyberattack would have on the country as well as gaps and vulnerabilities in America's preparedness for an energy infrastructure cyberattack.[61] It appears, however, that America's focus on energy cybersecurity stops short of natural gas pipelines. Though the threat to natural gas pipeline cybersecurity is prevalent, acknowledged, and increasingly serious, cybersecurity for natural gas pipelines is not yet prioritized.

IV. CYBERSECURITY THREATS TO NATURAL GAS PIPELINES

While the above cyberattacks were on the electric gird and not specifically natural gas pipelines, the interdependency between natural gas pipelines and the electric grid is steadily increasing.[62] Thus the cyber vulnerabilities of natural gas pipelines are important in their own right and even more so because of the effect that the vulnerabilities have on the electric power sector as a whole.[63] DOE reported in 2017 that the electric sector is increasingly reliant on gas-fired energy: in 2005 natural gas accounted for 9% of the United States' electricity generation, grew to 30% by 2013, and reached

---

[59] *Id.*

[60] *Id.* While trial runs of worst-case scenario reboots have worked, Weiss has expressed serious concern over how "fragile and prone to disruption" a recovery effort might be. *Id.*

[61] Exec. Order No. 13800, 82 Fed. Reg. 22, 391 (2017).

[62] 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/D2WT-RP4V].

[63] *Id*.

42% by 2016.[64] As natural gas has "become a major part of the fuel mix" the urgency of pipeline cybersecurity threats has increased.[65]

A. Methods of Cyberattacks on Natural Gas Pipelines

Natural gas pipelines have moved to computerized systems, which are vulnerable to cybersecurity threats. Most pipelines use the Supervisory Control and Data Acquisition ("SCADA") systems.[66] SCADA collects real-time data to provide the pipeline operator with "feedback and information about the entire pipeline system and triggers safety alarms when operating conditions are not within the prescribed design parameters."[67] In turn, operators can remotely send commands to control the variables measured and reported by SCADA.[68]

While SCADA is useful to pipelines in that they can reduce operating costs and increase system efficiency, SCADA can cause destruction even without an outside adversary.[69] For example, the San Bruno pipeline explosion, which killed eight people, injured fifty-eight others, and destroyed thirty-eight homes was a result of "erroneous and unavailable SCADA pressure readings."[70] Natural gas pipeline explosions resulting from faulty SCADA readings and signals also occurred in Bellingham, Washington and Texas City,

---

[64] Meg Handley, *Is the U.S. Too Dependent on Natural Gas for Electricity?,* U.S. NEWS (Mar. 28, 2013), https://www.usnews.com/news/articles/2013/03/28/is-the-us-too-dependent-on-natural-gas-for-electricity [https://perma.cc/6LYX-2WC3]; *Natural Gas Generators Make Up the Largest Share of Overall U.S. Generation Capacity,* U.S. ENERGY INFO. ADMIN. (Dec. 18, 2017), https://www.eia.gov/todayinenergy/detail.php?id=34172 [https://perma.cc/RR9H-NYAZ].

[65] Tarallo, *supra* note 62.

[66] Dancy & Dancy, *supra* note 32, at 584.

[67] *Id*. at 585. SCADA monitors and provides information such as the pipeline pressures, temperatures, tank levels, and pump seeds. *Id.*

[68] *Id*.

[69] *Id*.

[70] *Id*. at 586. The pipeline explosion in Bellingham, Washington resulted from the faulty of the SCADA system and caused spillage of 237,000 gallons of gasoline into a creek, which ignited. The explosion killed and injured a number of people and caused $45 million in damage. The Texas City explosion was caused by faulty SCADA signals and also resulted in a number of death and significant injuries. *Id*.

Texas, both of which resulted in loss of life.[71] SCADA is also becoming increasingly vulnerable to cyberattacks that could increase these deadly accidents.[72]

The Congressional Research Service states "cyber infiltration of [SCADA] 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."[73] In other words, adversaries could capitalize on the damage SCADA is already capable of executing and manipulate the system to result in more death and destruction.[74]

There are a variety of other methods that an adversary could use to threaten the cybersecurity of a natural gas pipeline.[75] For example, attackers can infiltrate an organization's operation systems through a communication pathway such as the internet to "disrupt its service and cause spills, releases, explosions, or fires."[76] Another potential avenue to conduct a cyberattack is through spear-phishing.[77] Adversaries can also access and infiltrate the control valves, pressure monitors, and other equipment that are connected to wireless networks, which are vital to the pipelines functioning.[78]

B. Examples of Natural Gas Pipeline Attacks

While the U.S. has not experienced a cyberattack that has caused physical damage to natural gas pipelines, foreign pipelines have

---

[71] *Id*.
[72] *See id*. at 585.
[73] PAUL W. PARFOMAK, CONG. RESEARCH SERV., R42660, PIPELINE CYBERSECURITY: FEDERAL POLICY ii (2012).
[74] *See id.*
[75] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 5, at 13.
[76] *Id*.
[77] *Id*.
[78] *See* Krauss, *supra* note 35; U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 5, at 12. Cyberattacks are not limited to gas disruption or explosion, but instead cyberattacks can allow an adversary to access confidential customer and business data such as "holdings, trading strategies and exploration and production technologies." A hacker can also issue fake transactions and potentially "jumble gas shipments." A cyberattack can also result in operation disruptions, modification or destruction or private information, and be an overall threat to national security. *Id.*

been damaged at the hands of cyberattackers. For example, in 1982 the Trans-Siberian pipeline, which runs over much of Russia, experienced a significant explosion.[79] A "malicious code" in the pipeline control software caused the explosion by increasing the pipeline pressure.[80] The explosion equaled that of a nuclear weapon.[81]

In 2008, the Baku-Tbilisi-Ceyhan pipeline, which spans from the Caspian Sea to the Turkish Mediterranean coast and is outfitted with "sensors and cameras to monitor every inch of the line" exploded without triggering any alarms or cameras.[82] The mystery source of the explosion turned out to be a "sophisticated cyberattack on the pipeline's control system."[83] Though the source of the attack is not definitively known, attackers tied to the Russian government were able to access the pipeline computer system through the surveillance cameras and cost billions of dollars in lost tariffs and export revenue.[84] While the exact capabilities of the attackers are also not known, the pipeline had just installed new cameras that possessed communication software vulnerable to attacks.[85] It was reported that the vulnerabilities were exploited and the attackers gained entry onto the network through the computers.[86] The attackers were also said to have intruded into the alarm server through a Windows operating system containing malicious software.[87]

Cyberattacks on U.S. natural gas pipelines are not just a possibility, but America's natural gas pipelines have already experienced a number of cyberattacks. For example, DHS and FBI have found that Russia has already "infiltrated the U.S. electric grid, embed[ded] malware that could incapacitate power plants,

---

[79] Dancy & Dancy, *supra* note 32, at 587.
[80] *Id*.
[81] *Id*. at 588.
[82] *Id*.
[83] *Id*.
[84] Robert M. Lee et al., *Media report of the Baku-Tbilisi-Ceyhan (BTC) pipeline Cyber Attack*, INDUS. CONTROL SYS. 3 (Dec. 20, 2014); Dancy & Dancy, *supra* note 32, at 588–89.
[85] Lee et al., *supra* note 84, at 3–4.
[86] *Id*. at 4.
[87] *Id*.

pipelines, and water supplies, and . . . ha[s] even gained access to power plant control rooms."[88] In 2012, specifically, Industrial Control Systems Cyber Emergency Response Team identified a number of cyber intrusions that targeted natural gas pipelines, which were traced back to a "single campaign with spear-phishing activity."[89] In 2018, a cyberattack in Houston, Texas did not disrupt gas service but "forced four of the nation's natural-gas pipeline operators to temporarily shut down computer communications with their customers."[90] More recently in 2019, a firewall was "exploited" at a western U.S. utility, which caused devices to reboot and communication disruptions.[91]

C. Natural Gas Pipelines Cyber Warfare

In response to these attacks and even larger vulnerabilities, the U.S. is taking actions that "are potential game changers in the global escalation of cyber warfare."[92] The U.S. is on "cyberwar footing" with Iran's military command and control networks and Russia's electric grid.[93] For example, the U.S. has imbedded computer codes that are "the digital equivalent of bombs that could be detonated" throughout Russia's electric grid.[94] Moreover, in June 2019, President Donald Trump ordered a cyberstrike against the Islamic Revolutionary Guard Corps that disabled Iranian computer systems that were posed to attack oil tankers in the Persian Gulf.[95]

---

[88] Shkor & Connors, *supra* note 53.
[89] MONTHLY MONITOR, INDUS. CONTROL SYS. CYBER EMERGENCY RESPONSE TEAM 1 (2012).
[90] Krauss, *supra* note 35.
[91] HJ Mai, *NERC Finds First Remote Hacker Interference on US Grid from Cyberattack*, UTILITY DIVE (Sept. 9, 2019), https://www.utilitydive.com/news/nerc-finds-first-remote-hacker-interference-on-us-grid-from-cyberattack/562478/ [https://perma.cc/6CQK-NCXJ].
[92] Shkor & Connors, *supra* note 53.
[93] *Id*.
[94] *Id*.; *see also* 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/C99Q-T6ZP].
[95] Ellen Nakashima, *Trump Approved Cyber-strikes Against Iranian Computer Database Used to Plan Attacks on Oil Tankers*, WASH. POST (June 22, 2019), https://www.washingtonpost.com/world/national-security/with-trumps-approval-

These are examples of offensive cyber warfare tactics and show cyberattacks are now used as an active war tool and have been formally weaponized. These offensive efforts also increase the likelihood of a counterattack, exacerbating the need for the U.S. to bolster energy infrastructure cybersecurity.[96] In 2008, the Department of Defense sought to strengthen U.S. energy cybersecurity through the creation of the U.S. Cyber Command.[97] Cyber Command's job is to direct, synchronize, and coordinate "cyberspace planning and operations in defense of the U.S. and its interests."[98] President Trump's 2020 budget also requested $9.6 billion for cyber defense and offensive operations through Cyber Command.[99]

Cyber Command is a reaction to the cyber-intrusions and cyberattacks that threaten America's energy infrastructure. America's natural gas pipelines, however, remain vulnerable because of a lack of any meaningful regulation or protection.[100] Natural gas pipelines' main weakness is that the regulatory framework that governs the infrastructure's cybersecurity is ineffective. TSA is the regulatory body that oversees natural gas pipeline cybersecurity, but they have promulgated only voluntary guidelines, which impose no actual requirements on natural gas pipelines.[101]

Though cyber-intrusions have not yet resulted in physical damage or death, the current regulatory framework is not sufficient to prevent against the growing threat of a cyberattack on natural gas pipelines. TSA has no way to "ensure that its guidelines reflect the

---

pentagon-launched-cyber-strikes-against-iran/2019/06/22/250d3740-950d-11e9-b570-6416efdc0803_story.html [https://perma.cc/554K-9DNY]; Shkor & Connors, *supra* note 53.

[96] Shkor & Connors, *supra* note 53.

[97] *History*, U.S. CYBER COMMAND, https://www.cybercom.mil/About/History/ (last visited Nov. 30, 2019) [https://perma.cc/MJQ7-CXBQ].

[98] *Id*.

[99] Aaron Boyd, *Trump's 2020 Budget Requests About $11 Billion for Cyber Defense and Operations*, NEXTGOV (Mar. 11, 2019), https://www.nextgov.com/cybersecurity/2019/03/trumps-2020-budget-requests-about-11-billion-cyber-defense-and-operations/155445/ [https://perma.cc/W5C6-6FEE].

[100] HOMELAND SECURITY ISSUES IN THE 116TH CONGRESS, *supra* note 30, at 2.

[101] TRANSPORTATION SECURITY ADMIN., *supra* note 6.

latest known standards and best practices for physical security and cybersecurity, or address the dynamic security threat environment that pipelines face."[102]

Cyber-threats evolve with technology to become more deadly and destructive. As the threats evolve, cybersecurity regulations need to rise to meet them, which current regulations are unable to do.[103] TSA lacks the resources necessary to strengthen and enforce mandatory guidelines making TSA unlikely to implement mandatory regulations and similarly renders TSA the wrong agency to promulgate mandatory regulations. Rather, DOE should promulgate natural gas pipeline cybersecurity regulations.

V. CURRENT REGULATIONS OF NATURAL GAS PIPELINES

Over time, natural gas extraction, production, and mobility has been regulated by a number of different agencies.[104] While local governments originally regulated the natural gas markets, the natural gas business possessed many of the characteristics of a natural monopoly, making it a prime product for federal regulation.[105] In other words, one "distribution network could deliver natural gas more cheaply than two companies with overlying distribution networks and markets."[106] Further, the natural gas industry was "clothed in the public interest" in that people needed access to cheap, reliable natural gas.[107]

In exchange for the ability to operate as a monopoly, natural gas had to accept heavy regulation to prevent the industry from taking

---

[102] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 5.
[103] *See id.*
[104] *The History of Regulation*, NATURALGAS.ORG (Sept. 20, 2013), http://naturalgas.org/regulation/history/ [https://perma.cc/8GEW-ZDZM].
[105] *See id.* Electricity is a prominent example of a natural monopoly whereby it is considered cheaper and more efficient for a single company to deliver natural gas than two companies. A natural monopoly grants total control over the market, without competition, which leaves the monopoly in a prime spot to take advantage of its position. To prevent a monopoly from abusing its market power, rates are regulated by governments. Regulation requires that "just and reasonable" rates are set so as to not take advantage of consumers. *Id.*
[106] *Id*.
[107] *Id*.; *see* KARL MCDERMOTT, COST OF SERVICE REGULATION IN THE INVESTOR-OWNED ELECTRIC UTILITY INDUSTRY 4 (2012).

advantage of its exclusive position, known as the regulatory compact.[108] Today, a number of different agencies regulate the various aspects of natural gas. TSA, housed within DHS, oversees natural gas pipeline security.[109] The Pipeline and Hazardous Material Safety Administration ("PHMSA"), a sub-agency of the Department of Transportation ("DOT"), as well as DOE play a role in response and recovery if a natural gas pipeline cybersecurity incident or intrusion occurs.[110]

A. Federal Regulation of Natural Gas Markets

Local regulation was effective during the early days of natural gas.[111] By the early 1900s, however, local regulation became more difficult as natural gas was distributed between municipalities and local governments no longer oversaw the entire natural gas distribution chain.[112] State governments intervened and began to regulate natural gas distribution through public utility commissions and public service commissions.[113]

Technology, however, developed to allow natural gas to be transported between states.[114] The U.S. Supreme Court's "Commerce Clause Cases" held that state regulation of natural gas pipelines violated the interstate commerce clause.[115] As a result of the decision, state governments could no longer regulate interstate pipelines but, at the time of the decision, no federal legislation addressed interstate pipelines.[116]

Congress responded to this gap with the passage of the Natural Gas Act ("NGA") of 1938.[117] Finally, the federal government,

---

[108] *See* MCDERMOTT, *supra* note 107.
[109] Dancy & Dancy, *supra* note 32, at 598.
[110] *See* TRANSPORTATION SECURITY ADMIN.: PIPELINE SECURITY AND INCIDENT RECOVERY PROTOCOL PLAN 1 (2010).
[111] *The History of Regulation, supra* note 104.
[112] *Id*.
[113] *Id*.
[114] *Id*.
[115] *Id*.
[116] *Id*.
[117] Public Utility Holding Company Act of 1935, 15 U.S.C. § 79 (a) (2012); *Natural Gas Act of 1938,* U.S. ENERGY INFO. ADMIN.,

through the Federal Power Commission ("FPC") could directly regulate interstate natural gas.[118] FPC also had the authority to approve any new interstate pipelines.[119] In 1954, because of the U.S. Supreme Court's decision in *Phillips Petroleum Co. v. Wisconsin*[120], wellhead prices were also brought under FPC regulation, granting FPC more control over natural gas pipelines.[121]

While the NGA filled a regulatory gap, the Act was disastrous for America's natural gas market and resulted in a 1978 natural gas shortage.[122] In response, FPC was reorganized into the Federal Energy Regulatory Commission ("FERC") and Congress enacted the Natural Gas Policy Act to create a "single national natural gas market" regulated under FERC.[123]

Today, FERC is the main authority in natural gas pipeline market regulation.[124] However, FERC plays no role in natural gas

---

https://www.eia.gov/oil_gas/natural_gas/analysis_publications/ngmajorleg/ngact1938.html [https://perma.cc/2PHY-LB3M].

[118] *Natural Gas Act of 1938*, *supra* note 117.

[119] *Id*.

[120] Philips Petroleum Co. v. Wisconsin, 347 U.S. 672, 685 (1954).

[121] *The History of Regulation*, *supra* note 104. Wellhead prices were unregulated after the Natural Gas Act because the Act did not institute regulatory sales of natural gas from producers to pipelines. Wellhead prices are "the rate at which producers [sell] natural gas into the interstate market[.]" *Id*.

[122] *Id*. FPC initially set rates based on cost of production but this became a heavy administrative burden on the FPC due to the large number of different natural gas producers. FPC moved to set rates on an individual basis whereby rates were set on each producer's cost of service. Again, administratively burdensome, even impossible and resulted in enormous backlog. As a result, FPC moved to set rates based on geographic areas by dividing the U.S. into five producing regions where rates were set with interim ceiling prices. Again, became infeasible and FPC adopted national price ceilings. These different pricing systems were disastrous for the America's natural gas market and only the producing states had access to natural gas while consuming states experienced natural gas shortages. *Id*.

[123] Natural Gas Policy Act of 1978, 15 U.S.C. § 207(a)(3) (2012); *The History of Regulation*, *supra* note 104; *History of FERC*, FED. ENERGY REGULATORY COMM'N, https://www.ferc.gov/students/ferc/history.asp (last visited Nov. 30, 2019) [https://perma.cc/UGP5-2CN5].

[124] *See Natural Gas Pipelines*, FED. ENERGY REGULATORY COMM'N (Aug. 2015), https://www.ferc.gov/industries/gas/indus-act/pipelines.asp [https://perma.cc/T5HT-7K9E].

pipeline safety or security.[125] Rather, FERC works with other agencies that oversee various aspects of natural gas pipeline safety and security.[126]

B. Natural Gas Pipeline Security Oversight: TSA

The primary agency charged with natural gas pipeline security responsibilities is TSA.[127] After the September 11, 2001 attacks, the Aviation and Transportation Security Act established TSA to oversee the security of all modes of transportation under DOT.[128] A year later, the Homeland Security Act of 2002 transferred TSA from DOT to DHS where it remains today.[129]

To comply with their security responsibilities, TSA maintains the Pipeline Security Division, which "works to develop security measures to mitigate risk, monitor compliance with security guidelines, and build and maintain stakeholder relations."[130] TSA also possesses the authority to issue physical and cybersecurity regulations for natural gas pipelines.[131] However, the agency has declined to issue new rules or regulations to address natural gas pipeline security since 9/11.[132] In reality, no bright line regulations have ever been issued by TSA.[133] Instead, TSA has issued a series of guidelines—specifically the Pipeline Security Guidelines—which were updated in 2018 for the first time since 2011.[134]

---

[125] *Id.*
[126] *Id*.
[127] Dancy & Dancy, *supra* note 32, at 598.
[128] Aviation and Transportation Security Administration Act, 49 U.S.C. § 114(d)(2) (2001).
[129] Homeland Security Act of 2002, 6 U.S.C. § 203 (2) (2012); Dancy & Dancy, *supra* note 32, at 598.
[130] TRANSPORTATION SECURITY ADMIN., *supra* note 110, at 5.
[131] Dancy & Dancy, *supra* note 32, at 598.
[132] Troutman Sanders Pipeline Practice, *Pipeline Security and Cybersecurity: Are Guidelines Enough to Protect Critical Infrastructure?*, TROUTMAN SANDERS (June 4, 2018), https://www.pipelaws.com/2018/06/pipeline-security-cybersecurity-guidelines-enough-protect-critical-infrastructure/ [https://perma.cc/CM7C-48J7].
[133] *See* Dancy & Dancy, *supra* note 32, at 598.
[134] PIPELINE SECURITY GUIDELINES, *supra* note 6, at 1.

The Pipeline Security Guidelines lay out a "Corporate Security Program" and encourage pipeline operators to establish and implement the program.[135] The program's key recommendations are to develop a corporate security plan, which should identify who will execute the plan, document the company's security policies in reference to other companies' policies, and be reviewed on an annual basis as well as provided to TSA for review.[136]

The Pipeline Security Guidelines also promulgate recommendations for natural gas pipeline cybersecurity measures based off of the National Institute of Standards and Technology ("NIST")'s "Framework for Improving Critical Infrastructure Cybersecurity."[137] NIST's framework sets "standards and best practices to assist organizations in managing cybersecurity risks" and "promote the protection of critical infrastructure."[138] TSA's Pipeline Security Guidelines recommend that organizations follow NIST's cybersecurity framework and list a number of industry and federal government entities for pipeline operators to consult as a reference for cybersecurity programs.[139]

TSA's guidelines, however thorough, are simply advisory.[140] The guidelines encourage the natural gas industry to implement the suggested security measures, but again, implementation is only encouraged, not mandated.[141] Specifically, the guidelines state that they, "[do] not impose requirements on any person or company."[142] These voluntary standards essentially leave the industry self-regulated.[143]

---

[135] *Id*. at 2.
[136] *Id*. at 2–4.
[137] *Id*. at 16. NIST is not a Federal agency but an independent scientific entity and thus does not possess any regulatory authority. *Id.*
[138] *Id*.
[139] *Id*. at 21.
[140] Troutman Sanders Pipeline Practice, *supra* note 132.
[141] TRANSPORTATION SECURITY ADMIN., *supra* note 6, at 2.
[142] *Id*. at 1.
[143] Troutman Sanders Pipeline Practice, *supra* note 132.

C. Other Agencies that Play a Role in Natural Gas Pipeline Security

While TSA is the current entity set to oversee natural gas pipeline safety and security, its means for incident response and recovery are scant.[144] As a result, other agencies must play a role in natural gas pipeline safety and security.[145] In 2010, TSA issued a "Pipeline Security and Incident Recovery Protocol Plan," which detailed the roles different federal agencies play in the case of a security incident.[146]

As the energy specific agency, DOE plays a significant role in pipeline security response as the agency is "responsible for coordinating all activities related to energy infrastructure protection."[147] DOE is also responsible for the facilitation of assessments, reports, and restoration of "damaged energy systems and components."[148] During a natural gas pipeline emergency, DOE would coordinate with other federal agencies and the private sector to assess the supply of natural gas.[149]

TSA Assistant Secretary or Secretary of Homeland Security is also an active participant in the event of a pipeline security threat or incident. Either Secretary may deploy Visible Intermodal Prevention and Response ("VIPR") teams that work with local security and law enforcement and provide supplemental security.[150]

---

[144] *See* TRANSPORTATION SECURITY ADMIN., *supra* note 110, at 1.
[145] *See* Tarallo, *supra* note 62.
[146] *See* TRANSPORTATION SECURITY ADMIN., *supra* note 110, at 1.
[147] *Id*. at 7.
[148] *Id*. This responsibility is carried out by the Office of Electricity Delivery and Energy Reliability and the responsibility is specifically called Emergency Support Function ("ESF") 12. ESF12 is outlined by the National Response Framework, which is consistent with the Pipeline Security and Incident Recovery Protocol Plan. *Id.*
[149] *See id.*
[150] *Id*. at 6. "VIPR teams are comprised of Federal Air Marshals (FAMs), Federal Security Directors (FSDs), Surface Transportation Security Inspectors (STSIs), Transportation Security Officers (TSOs), Behavior Detection Officers, and Explosives Detection Canine teams." *Id.*

VIPR teams also provide pipeline companies "pre-incident deterrence measures" after a threat has been detected.[151]

The final key agency in natural gas pipeline security is PHMSA. Within PHMSA lies the Office of Pipeline Safety, which is responsible for ensuring the "safe, reliable, and environmentally sound operations of our nation's pipeline transportation system."[152] PHMSA oversees interstate pipelines once a project is operating through monitored compliance which ensures pipelines operate safely and securely.[153]

PHMSA seeks compliance with pipeline safety standards through pipeline inspections and investigation of safety incidents.[154] PHMSA can also provide assistance during response or recovery of a pipeline security incident through its Regional Emergency Transportation Coordinator.[155] DOT can also issue special permits, safety orders, and corrective action orders in response to incidents.[156]

Other agencies can provide support in different capacities in the event of a natural gas pipeline security incident. Federal Emergency Management Agency, can provide support and planning during an incident.[157] The Office of Infrastructure Protection within DHS coordinates efforts to reduce risk from terrorist activities.[158] The National Transportation Safety Board investigates pipeline

---

[151] *Id*. VIRP teams also provide "post-incident site security" if the "pre-incident deterrence measures" is not effective in preventing a detected threat. *Id.*
[152] *Safety Awareness Overview*, PIPELINE & HAZARDOUS MATERIALS SAFETY ADMIN. (June 11, 2019), https://www.phmsa.dot.gov/safety-awareness/pipeline/safety-awareness-overview [https://perma.cc/SE7D-YFFX].
[153] Jacquelyn Pless, *Making State Gas Pipelines Safe and Reliable: An Assessment of State Policy*, NAT'L CONFERENCE OF STATE LEGISLATURES (Mar. 2011), http://www.ncsl.org/research/energy/making-state-gas-pipelines-safe-and-reliable.aspx [https://perma.cc/7EJT-N6RA].
[154] TRANSPORTATION SECURITY ADMIN., *supra* note 110, at 6.
[155] *Id*. at 7. "Each RETCO manages regional DOT emergency preparedness and response activities in the assigned region on behalf of the Secretary of Transportation. RETCOs are responsible for coordinating with, and providing assistance to, other Federal agencies and State, local, and tribal governments." *Id.*
[156] *Id*.
[157] *Id*. at 8–9.
[158] *Id*.

transportation accidents unless the event becomes categorized as a criminal act, at which point the FBI would become involved.[159]

The above agencies all play a role in a natural gas pipeline cybersecurity incident or attack.[160] However, there is no concrete plan in place to ensure an attack does not occur, just general guidelines promulgated in the hopes the industry will rise to the standard. While a meticulous system with a detailed understanding of how to respond to an attack is undoubtedly useful and important, focus should be directed at preventing cyberattacks from occurring.

VI. NATURAL GAS PIPELINE CYBERSECURITY REGULATIONS SHOULD BE MANDATORY

In the United States, cyberattacks and impending cyber warfare on natural gas pipelines are a legitimate concern exacerbated by the federal government's ineffective oversight.[161] Despite pushes by policy makers to make the cybersecurity of natural gas pipelines a national security issue, security regulations currently remain voluntary guidelines.[162] The private sector, however, has advocated to keep natural gas pipeline cybersecurity standards voluntary.[163]

A. The Private Sector's Argument that Regulation Should Remain Voluntary

The private sector has argued that natural gas pipeline cybersecurity standards should remain voluntary and would prefer cybersecurity be regulated in a "risk-based approach augmented by public-private partnerships."[164] The private sector has four core arguments as to why mandatory regulations should not be enacted: (1) prescriptive regulations would "increase business expenses and overhead[;]" (2) companies would be forced to comply with measures that rapidly become "out-of-date and ineffective[;]" (3)

---

[159] *Id*. at 9.
[160] *Id*.
[161] *See* Christofaro, *supra* note 51.
[162] Tarallo, *supra* note 62.
[163] Chris Laughlin, Note, *Cybersecurity in Critical Infrastructure Sectors: A Proactive Approach to Ensure Inevitable Laws and Regulations are Effective*, 14 COLO. TECH. L.J. 345, 357 (2016).
[164] *Id*. at 356–57.

the already functional public-private partnership to address cybersecurity would be disincentivized; and (4) stricter "regulations would not necessarily improve cybersecurity."[165]

Specifically, natural gas pipeline trade organizations like the Interstate Natural Gas Association of America ("INGAA") believe that "effective collaboration," achieved through guidance rather than enforced regulations, is foundational to the security of natural gas pipelines.[166] INGAA claims that "[r]eal-time, actionable information is vital to ensure [that] pipeline operators are equipped with the latest intelligence on threats," which the pipeline industry already maintains through a network of information sharing.[167] INGAA further argues that mandatory regulations will corrode the effective relationship already in place between information sharing facilities and the oil and gas industry, TSA, and DHS.[168]

Other proponents of voluntary regulation, such as Dan Coats, the Director of National Intelligence, further argue mandatory regulations inhibit the flexibility that is required for the industry to "adapt and update protocols" in responses to cyberattacks.[169] Specifically, "[e]xperience shows that mandatory standards often are outdated almost as soon as they are introduced."[170] Rather than mandatory regulations, there should be "baseline practices" on which the industry can build "in a way that matches the nimbleness of [] adversaries."[171]

Voluntary guidelines are not unique to natural gas pipelines.[172] Other "privately held critical infrastructure," such as banks and telecommunications carriers, that would likely be targeted by a

---

[165] *Id*. at 357.
[166] Don Santa, *Congress should support efforts to further protect pipelines from cyber threats*, THE HILL (Feb. 28, 2019), https://thehill.com/opinion/cybersecurity/432024-congress-should-support-efforts-to-further-protect-pipelines-from-cyber [https://perma.cc/LX7D-DWQ6].
[167] *Id*.
[168] *Id*.
[169] *Id*.
[170] *Id*.
[171] *Id*.
[172] Nathan A. Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1506 (2013).

"large-scale cyber-attack" are left to private regulation.[173] Legal scholars have observed that the U.S. "follows a 'bifurcated approach to network security' that 'relie[s] predominately on private investment in prevention and public investment in prosecution.'"[174] In other words, for much of America's critical infrastructure, the government does not impose mandatory regulations and the companies are left alone to protect themselves, including their cyber-networks.[175]

These arguments are combatted by a recent trend that "regular firms that operate in a competitive market (such as online retailers) may be adequately protecting their systems against ordinary intruders" whereas "strategically significant firms in uncompetitive markets (such as power companies and other public utilities) seem less likely to maintain defenses capable of protecting their systems against skilled and determined adversaries (such as foreign intelligence services)."[176] As a result, while some members of the private industry may be equipped to handle the cyber-threats posed to firms in regulated markets, the private industry has not adequately protected natural gas pipelines.

Even more notably, cyber-security is often overlooked by private industry when left to regulate itself.[177] Rather, the cyber-security field is "primarily concerned with negative externalities. Just as firms tend to underinvest in pollution controls because some costs of their emissions are borne by those who are downwind, they also tend to underinvest in cyber-defense because some costs of intrusions are externalized onto others."[178] The full cost of a cyberattack is not borne by the energy company, but is instead borne by the public at large who relies on the granted monopoly industry for an essential service, de-incentivizing energy companies to invest in the required defense mechanisms absent some mandatory regulation.[179]

---

[173] *Id*.
[174] *Id*.
[175] *Id*.
[176] *Id*. at 1506–07.
[177] *See id*. at 1508.
[178] *Id*.
[179] *Id*.

B. Argument that Natural Gas Pipeline Regulations Should Be Mandatory

Self-regulation may be sufficient for other private industries, but natural gas' unique situation requires mandatory regulation to defend against pipeline cyberattacks. FERC Commissioner, Richard Glick, has spoken out about the weakness of these voluntary guidelines and states, "[i]f you just have one weak link—one entity that does not follow voluntary standards—it can cause significant damages."[180] Unfortunately, "America's interest in protecting our critical infrastructure from national security threats is in tension with America's interest in allowing the private sector to provide many essential services in critical infrastructure sectors."[181] However, with the U.S. openly engaged in "offensive cyber intrusions" against foreign nations, it is imperative to recognize and address the weaknesses in U.S energy cybersecurity.[182]

It is an anomaly that the cybersecurity of natural gas pipelines has been left to market forces and voluntary action.[183] After 9/11 the U.S. government moved from deregulation and privatization towards tightened regulations to strengthen homeland security.[184] It is difficult to leave national defense and homeland security to market influences.[185]

> National defense and homeland security are public goods where individuals share in the benefits irrespective of how much they spend [if at all]. Markets are inefficient at supplying goods and services in situations where groups of people must work together to achieve a good outcome but the incentive for investment and cooperation is low. In these situations, the private sector will not produce an optimal outcome.[186]

The private sector controls a majority (85%) of "cyber relevant critical infrastructure in the U.S." and while the private sector has a great interest in protecting that infrastructure from cyberthreats,

---

[180] Troutman Sanders Pipeline Practice, *supra* note 132.
[181] Laughlin, *supra* note 163, at 351.
[182] *Id*.; s*ee* Shkor & Connors, *supra* note 53.
[183] *See* JAMES A. LEWIS, AUX ARMES, CITOYENS: CYBER SECURITY AND REGULATION IN THE UNITED STATES 1 (Elsevier's Telecommunications Policy, 2005).
[184] *Id*.
[185] *Id*.
[186] *Id*.

those "may not align exactly with the interests of the government or the public."[187] For example, specific individual companies may not believe they will be the target of a foreign cyberterrorist act.[188] As a result, that individual company may calculate that it is not in its best interest to protect against a hypothetical, seemingly unlikely attack.[189] The government may see it in the opposite light in that an unsuspecting utility is the exact target for an adversary.[190]

These interests are further exemplified when private businesses employ cost-benefit analyses.[191] If the cost to protect a company from a cyberattack is outweighed by the cost of recovery after an attack, the company is unlikely to employ the security measure.[192] Companies are further discouraged from investing in security measures because the company does not fully "internalize the negative and positive externalities of a successful cyberattack."[193] For example, a company will internalize the cost of new computers, new infrastructure, and lost revenue in the wake of a cyberattack but the government will assist in finding the culprit and get the computers operational.[194]

In other industries, insurance has served as an implicit regulator, and has been used as a "tool to 'outsource' public regulations" in industries without full governmental regulation.[195] Insurance may function as a form of private regulation, governing how organizations handle risks.[196] As a result, insurance can prevent and

---

[187] Laughlin, *supra* note 163, at 351.
[188] *Id*. at 352.
[189] *Id*.
[190] *Id*.
[191] *Id*. at 357.
[192] *Id*.
[193] *Id*. at 358.
[194] *Id*.
[195] Qihao He & Michael Faure, *Regulation by Catastrophe Insurance: A Comparative Study*, 25 CONN. INS. L.J. 189, 190 (2019). This article does not address how insurance can regulate the natural gas industry specifically but rather discusses five insurance-based regulatory tools ("risk-based pricing, contract design, loss prevention services, claim management, and refusal to insure") can generally reduce risk and loss from a catastrophic event. *Id*. at 189.
[196] *Id*. at 190–94. Regulation by insurance is not the same as insurance regulation. This paper refers to regulation by insurance.

mitigate losses associated with various risks such as external catastrophes.[197] Regulation through insurance can also incentivize organizations to protect themselves against disasters and catastrophic risks.[198]

Through techniques such as risked-based pricing, contract design, loss prevention, claim management, and refusal to insure, insurance can regulate potentially devastating events.[199] Insurance has been an effective implicit regulator in some industries, such as automobile, workplace, environmental, and medical liability.[200] Insurance has prevented environmental accidents, protected against flood and hurricane damage and combated climate-related extremes.[201] However effective in other industries, insurance has not filled the regulatory gap of natural gas pipeline cybersecurity because the insurance companies perceive the inadequate TSA guidelines as "best industry practice."[202]

Ultimately, federal mandatory regulation is necessary and inevitable.[203] The private industry is not able to regulate effectively and insurance cannot act as an implicit regulator.[204] While energy infrastructure has not yet experienced a deadly or severely destructive event from a cybersecurity breach, the threat is very real as has been demonstrated by a number of real-world examples.[205] Historical examples have shown that when the U.S. is attacked, the nation responds with legislation.[206] However, instead of waiting for

---

[197] *Id*. at 191.
[198] He & Faure, *supra* note 195, at 197.
[199] *Id*. at 201–07.
[200] *See* Tom Baker & Rick Swedloff, *Regulation by Liability Insurance: From Auto to Lawyers Professional Liability*, 60 UCLA L. REV. 1412, 1416–17 (2013).
[201] He & Faure, *supra* note 195, at 196–98.
[202] Troutman Sanders Pipeline Practice, *supra* note 132.
[203] Laughlin, *supra* note 163, at 351. There is an argument that natural gas pipeline cybersecurity should be regulated by the states. However, that discussion is outside the scope of this paper.
[204] Sales, *supra* note 172, at 1508.
[205] Laughlin, *supra* note 163, at 346–48.
[206] *Id*. at 346. For example, after Pearl Harbor, Congress passed the "National Security Act of 1947," Congress passed the "Antiterrorism and Effective Death Penalty Act of 1996" in response to the Oklahoma City and 1993 World Trade

the inevitable attack, the U.S. should promulgate mandatory regulations to prevent an attack on the country's natural gas pipelines.

VII. THE DEPARTMENT OF ENERGY SHOULD HAVE THE ABILITY TO REGULATE NATURAL GAS PIPELINE CYBERSECURITY

Updated and mandatory cybersecurity regulations for natural gas pipelines have been advocated for by a number of groups. The Government Accountability Office issued a report that accurately described TSA's guidelines as insufficient and, even though reissued in 2018, outdated because a number of critical areas were not revised.[207] TSA's Pipeline Security and Incident Recovery Protocol Plan has also not been updated since its issuance in 2010.[208] Further, TSA has no current plans to revise pipeline security threats, such as cybersecurity threats.[209]

A. TSA Should Not be the Agency to Promulgate Mandatory Natural Gas Pipeline Cybersecurity Regulations

According to FERC Chairman, Neil Chatterjee, and FERC Commissioner, Richard Glick, natural gas pipelines "must comply with mandatory standards" to "protect against attacks that could compromise electric service."[210] The two FERC leaders, however, do not advocate that TSA, the primary agency to oversee natural gas

---

Center bombings, and the "USA PATRIOT Act" was passed after the terrorist attack of 9/11. *Id.*

[207] *See generally*, U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-19-426, CRITICAL INFRASTRUCTURE PROTECTION: KEY PIPELINE SECURITY DOCUMENTS NEED TO REFLECT CURRENT OPERATING ENVIRONMENT (2019). The GAO found the guidelines did not revise in "three key areas; pipeline security threats, […] incident management policies, and DHS's terrorism alert system." *Id.*

[208] *Id*.

[209] *Id*.

[210] Neil Chatterjee & Richard Glick, *Cybersecurity threats to U.S. gas pipelines call for stricter oversight*, AXIOS (June 11, 2018), https://www.axios.com/cybersecurity-threats-to-us-gas-pipelines-call-for-stricter-oversight-09fac6e5-da94-491e-9523-d08ef15237f4.html **[**https://perma.cc/GL2D-S6FU**]**.

pipeline cybersecurity, should be the agency to implement mandatory regulations.[211]

Practically, TSA is not equipped to implement and enforce mandatory regulations.[212] As of May 2017, TSA had a mere six full-time employees in charge of security oversight for the millions of miles of pipelines, equating to approximately 450,000 miles of pipeline per employee.[213] Of these employees, none have "the specialized computer system expertise needed to support more extensive cybersecurity activities."[214]

TSA has not even kept up with the limited guidelines they have implemented. To assess pipeline vulnerabilities, TSA is supposed to conduct pipeline security reviews, known as Corporate Security Reviews ("CSRs") and Critical Facility Security Reviews.[215] However, TSA's limited number of staff has prevented TSA from conducting an appropriate amount of reviews.[216] In order to effectively review the "top 100 critical pipeline systems," a TSA priority, TSA would need to conduct 46 CSRs.[217] However, in 2018 TSA officials stated that their goal was to conduct between 15-23 CSRs per year.[218] TSA has not risen to meet its stated goal as in 2012 and 2013, only 14 full reviews were conducted, and only one was conducted in 2014.[219]

B. The Department of Energy is the Appropriate Agency to Promulgate Mandatory Natural Gas Pipeline Cybersecurity Regulations

TSA is not equipped to implement and enforce mandatory natural gas pipeline cybersecurity regulations. To oversee the

---

[211] *Id*.
[212] *Id*.
[213] *Id*.
[214] PARFOMAK, *supra* note 73, at 8–9.
[215] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 5, at 37.
[216] *Id*.
[217] *Id*. at 39 ("The TSA prioritizes reviewing and collecting information on the nation's top 100 critical pipeline systems.").
[218] *Id*. TSA officials stated their goal was to review "each pipeline company every 2 to 3 years; this would equate to about 15 to 23 CSRs per year." *Id.*
[219] *Id*. at 38.

security of all U.S. transportation is a tall order and TSA simply does not have the resources devoted to protecting natural gas pipelines from the cyberthreats they face. Congress, various federal agencies and the executive branch have all indicated, however, that DOE is the agency to implement stronger natural gas cybersecurity measures.[220] DOE already plays an active role in pipeline security and incident response and should move into the position of being the primary preventative agency by implementing mandatory regulations.[221]

Congress has taken note of natural gas pipeline cybersecurity threats. Fred Upton, a Representative from Michigan, stated "[w]e know that Russian agents and other nation states are waging cyber war on our energy infrastructure. It's critical to address these threats."[222] Members of Congress from both the Democratic and Republican parties have taken steps to tighten pipeline cybersecurity, but Congress has not directed legislation towards TSA.[223] It appears that Congressional advocates of stronger natural gas pipeline cybersecurity regulations think DOE is best equipped to promulgate cybersecurity rules as representatives have introduced a number of bills that direct cybersecurity initiatives to DOE, not TSA.[224]

The Pipeline and Liquified Natural Gas Facility Cybersecurity Preparedness Act ("H.R. 370") is one of the most prominent bills in

---

[220] *See* Rebecca Kern *Looming Cybersecurity Battle: Who Protects U.S. Pipelines?*, BLOOMBERG ENV'T (June 22, 2018), https://news.bloomberg environment.com/environment-and-energy/looming-cybersecurity-battle-who-protects-us-pipelines-corrected [https://perma.cc/4Z99-VR98]; Sobczak, *supra* note 7.

[221] TRANSPORTATION SECURITY ADMIN., *supra* note 110, at 7.

[222] Josh Paciorek, *News: Upton Statement after Energy Subcommittee Passes Bipartisan Pipeline and LNG Facility Cybersecurity Preparedness Act*, CONGRESSMAN FRED UPTON (May 16, 2019), https://upton.house.gov/news/documentsingle.aspx?DocumentID=401201 [https://perma.cc/84Q3-MKX6].

[223] Sobczak, *supra* note 7.

[224] *See generally* Cyber Sense Act of 2019, H.R. 360, 116th Cong. (2019); Energy Emergency Leadership Act, H.R. 362, 116th Cong. (2019); Enhancing Grid Security through Public-Private Partnership Act, H.R. 359, 116th Cong. (2019); Pipeline and LNG Facility Cybersecurity Preparedness Act, H.R. 370, 116th Cong. (2019). *Id.*

the slew of pipeline cybersecurity legislation. Introduced by U.S. Representative Fred Upton, H.R. 370 is a step towards tightening energy infrastructure's physical and cybersecurity guidelines by requiring DOE to establish policies and procedures that would ensure the security of natural gas pipelines.[225] H.R. 370 seeks to ensure the "security, resiliency, and survivability of natural gas pipelines" by establishing policies and procedures that coordinate states, federal agencies, and the energy sector.[226]

H.R. 370 calls for the development of "advanced cybersecurity applications and technologies for natural gas pipelines."[227] This would include performing "pilot demonstration projects . . . with representatives of the energy sector," creating "workforce development curricula," and providing "technological tools to help the energy sector voluntarily evaluate, prioritize, and improve physical security and cybersecurity capabilities of natural gas pipelines."[228] While the Bill represents a step towards mandatory regulation, it still leaves some regulatory efforts voluntary.[229] The Bill calls for the development of advanced cybersecurity applications and technology but only for *voluntary* use.[230] Similarly, H.R. 370 aims to "provide technical tools to help the energy sector *voluntarily* evaluate, prioritize, and improve physical security and cybersecurity capabilities."[231]

Statutory interpretation would suggest that only those two specific provisions are voluntary, while the remaining provisions are mandatory. In drafting H.R. 370, Congress specifically noted which provisions were voluntary by explicitly including the term

---

[225] Pipeline and LNG Facility Cybersecurity Preparedness Act, H.R. 370, 116th Cong. (2019). After being referred to the House's Subcommittee on Energy, H.R. 370 has last been ordered to be reported by voice vote. Fred Upton is currently a Congressman from Michigan's 6th District who served as Chairman of the Committee on Energy and Commerce from 2010-2016. H.R. 370 also includes security of hazardous liquid pipelines and liquefied natural gas facilities. *Id.*

[226] *Id*.

[227] *Id*.

[228] *Id*.

[229] *See id*.

[230] *Id*.

[231] *Id*. (emphasis added).

"voluntary."[232] As a result, it can be reasonably interpreted that in the absence of the term "voluntary," a provision is then mandatory.

H.R. 370 is surrounded by a host of other legislation from the 116th Congress concerning energy infrastructure's physical and cybersecurity, all directed at DOE. For example, H.R. 360, the Cyber Sense Act of 2019, would require the Secretary of Energy to "establish a voluntary Cyber Sense program to test the cybersecurity of products and technologies intended for use in the bulk-power system."[233]

Similarly, H.R. 362, the Energy Emergency Leadership Act, would amend the Department of Energy Organization Act to assign Assistant Secretaries new responsibilities in energy emergency response.[234] Assistant DOE secretaries would possess energy security functions such as "infrastructure, cybersecurity, emerging threats, supply, and emergency planning, coordination, response, and restoration. . ."[235]

Furthermore, H.R. 359, the Enhancing Grid Security through Public-Private Partnership Act, would require the Secretary of Energy to submit to Congress a report that assesses, among other things, "priorities, policies, procedures, and actions for enhancing the physical security and cybersecurity of electricity distribution systems to address threats to, and vulnerabilities of, such electricity distribution systems."[236] Like H.R. 370, H.R. 359 would require some voluntary actions from DOE such as providing voluntary implementation of electric grid utility cybersecurity assessments, but other provisions do not state that they are voluntary.[237] Under H.R. 359, some seemingly mandatory actions are to provide and assist with cybersecurity risk training to electric utilities, increase best practice sharing, and promote the cybersecurity of third-party vendors.[238]

---

[232] *Id*.
[233] Cyber Sense Act of 2019, *supra* note 224.
[234] Energy Emergency Leadership Act, *supra* note 224.
[235] *Id*.
[236] Enhancing Grid Security through Public-Private Partnership Act, *supra* note 223.
[237] *Id*.
[238] *Id*.

As described by Representative Upton and Energy and Commerce Committee Republican leader, Representative Greg Walden, "[t]hese bills reflect [the Energy and Commerce] Committee's commitment to strengthen energy delivery, security, and reliability for Americans. We are advancing legislation to bolster our protections against cybersecurity threats to energy infrastructure, which is key to the Department of Energy's emergency preparedness and response capabilities."[239] While these pieces of proposed legislation do not direct DOE to promulgate mandatory regulations, they are efforts to strengthen natural gas pipeline and electric grid cybersecurity and vest responsibilities in DOE.

FERC's Chairman Chatterjee and Commissioner Glick, also think DOE is the appropriate agency to implement mandatory regulations.[240] "Congress should vest responsibility for pipeline security with an agency that fully comprehends the energy sector and has sufficient resources to address this growing threat."[241] DOE certainly understands the energy sector. Further, DOE is the "Sector-Specific Agency for energy security" and has created an office for cybersecurity.[242]

The executive branch also appears to the think that DOE is the agency to tighten natural gas pipeline cybersecurity. The Trump Administration has announced that it is "establishing an office within the [DOE] to shore up cybersecurity for critical infrastructure like nuclear plants, refineries, and pipelines."[243] Now within DOE lies the Office of Cybersecurity, Energy Security, and Emergency

---

[239] Josh Paciorek, *News*: *Upton and Walden Statement on Full Committee Passage of Energy Bills*, CONGRESSMAN FRED UPTON (July 17, 2019), https://upton.house.gov/news/documentsingle.aspx?DocumentID=401248 [https://perma.cc/84WG-9ZA4].
[240] Chatterjee & Glick, *supra* note 210.
[241] *Id*.
[242] *Id*.
[243] Krauss, *supra* note 35.

Response, posed to "strengthen the DOE's ability to play a vital role protecting energy infrastructure from cyber threats . . . ."[244]

DOE has also stepped up to play a more active role in cybersecurity of the natural gas pipeline industry. DOE, not TSA is leading a "consortium over concerns industrial control systems" (private entities and key industries concerned with energy infrastructure cybersecurity threats).[245] The consortium is working together towards recommendations to increase natural gas pipeline cybersecurity.[246]

While the recommendations again would not be mandatory regulations, DOE has begun to come into a role whereby they can conduct pipeline oversight and eventually implement prescriptive regulations. As cyber-threats become more inevitable and as DOE obtains more authority over pipeline oversight, DOE should become the agency to issue mandatory regulation and be the agency to oversee the implementation of that regulation.

VIII. CONCLUSION

With the advancement of technology comes threats that were not previously of concern. Today, natural gas pipelines faces new cyber-threats that change and evolve rapidly. Cyberattacks on the energy grid have evolved into an active warfare tool and while the U.S. has not yet experienced a cyberattack that resulted in loss of life or serious infrastructure destruction, the U.S. is vulnerable and has still experienced relatively less significant cyber intrusions. While the U.S. has a history of passing reactive legislation after a significant event, America should proactively equip critical energy infrastructure with the tools they need to prevent and respond to a cyberattack.

---

[244] *Executive Order 13800 on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Assessment of Electricity Disruption Incident Response Capabilities*, DEP'T OF ENERGY (May 30, 2018).
[245] Dave Nyczepir, *DOE teams with industry on pipeline cyber*security, FED SCOOP (July 5, 2019), https://www.fedscoop.com/doe-industry-pipeline-cybersecurity-recommendations/ [https://perma.cc/9AAX-TTFL].
[246] *Id*.

The current regulatory framework to address cybersecurity threats to natural gas pipelines is a set of voluntary guidelines promulgated by TSA that simply encourage private industries to comply. However, these guidelines are insufficient and will likely be ineffective in the face of a serious cyberattack. The most effective mechanism to protect against a significant cyberattack is to require mandatory natural gas pipeline cybersecurity regulations.

TSA is not the agency that should promulgate mandatory regulations—the agency simply does not have the necessary resources, nor expertise. Rather, DOE, the agency over all of energy that already plays an active role in pipeline security, should implement mandatory guidelines. Congress has increased DOE's oversight of energy cybersecurity. President Trump has vested DOE with some cybersecurity authority and various agencies, including FERC, have advocated that DOE take the lead in pipeline cybersecurity regulations. DOE is coming into the role of pipeline cybersecurity oversight by beginning to work with the industry to update and increase pipeline cybersecurity, and the agency should continue this trend by promulgating mandatory cybersecurity regulations.