2023

# Cyber-Securing U.S. Critical Infrastrcure: The Colonial Pipeline Attack and What Can be Done to Protect Our Pipeline System

Bill Johnston

Cyber-Securing U.S. Critical Infrastrcure:

The Colonial Pipeline Attack and What Can be Done to Protect Our Pipeline System

Bill Johnston*

## I. INTRODUCTION

According to President Joe Biden, "[i]f we end up in a war . . . with a major power, it's going to be as a consequence of a cyber breach of great consequence."[1] The United States was hit with one such attack which shut down the country's largest gasoline pipeline.[2] On May 7, 2021, Colonial Pipeline was forced to cease operation of its 5,550-mile refined oil product pipeline after discovering it had been the victim of a ransomware attack.[3] In these types of cyberattacks, the hackers essentially "take computerized systems hostage until a payment is made."[4]

In response to the attack, Colonial Pipeline shut down the pipeline for fear that critical information could have been stolen and used to attack susceptible portions of the pipeline.[5] With its fuel delivery capabilities crippled, Colonial Pipeline CEO, Joseph Blount Jr., made the decision to pay the five million dollar ransom demanded by the hackers.[6] In explaining his decision, Mr. Blount said that "Colonial Pipeline would pay the ransom to have every tool available . . . to swiftly

---

* J.D. Candidate, 2023, Seton Hall University School of Law; B.A., University of Connecticut.

[1] Dustin Volz, *Biden Directs Agencies to Develop Cybersecurity Standards for Critical Infrastructure*, WALL ST. J. (July 28, 2021), https://www.wsj.com/articles/biden-directs-agencies-to-develop-cybersecurity-standards-for-critical-infrastructure-11627477200?mod=article_inline.

[2] Paola Rosa-Aquino & Chas Danner, *What We Know About the Colonial Pipeline Shutdown*, N.Y. MAG. (May 16, 2021), https://nymag.com/intelligencer/article/what-we-know-about-the-colonial-pipeline-shutdown-updates.html.

[3] *Id.*

[4] *Id.*

[5] David E. Sanger et al., *Cyberattack Forces a Shutdown of a Top U.S. Pipeline*, N.Y. TIMES (May 8, 2021), https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html.

[6] Christina Wilkie, *Colonial Pipeline Paid $5 Million Ransom One Day After Cyberattack, CEO Tells Senate*, CNBC (June 8, 2021), *https*://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html.

get the pipeline back up and running." According to the FBI, a hacker group believed to be operating inside of Russia, known as DarkSide, is responsible for the cyberattack.[7]

The United States is lucky that the attack was financially motivated instead of being driven by more sinister goals, such as terrorism. This point is illustrated by both the immediate impact and the possible negative outcomes that were avoided. Shortly after the attack, seventy-one percent of gas stations in North Carolina and forty-nine percent of gas stations in Georgia were without gasoline.[8] In the wake of the shortage, the average national price for gas reached its highest level since 2014.[9] The Department of Transportation declared regional states of emergency in response to the fuel shortage.[10] The shutdown of the pipeline caused panic-buying among U.S. citizens and forced airlines to alter travel schedules.[11] Despite all of these issues, the impact could have been much worse. If this attack had been carried out by another actor wishing to harm the critical infrastructure of the United States, the results could have been catastrophic for our economy, society, and environment. The Colonial Pipeline hack demonstrates that the President is right to fear that a large scale cyberattack could lead to war. As America's foreign wars wind down in the Middle East, national security demands a greater focus on defending the nation's critical infrastructure from cyberattacks.

---

[7] Ewan Palmer, *What is DarkSide? Russia-Linked Hacker Group Behind Colonial Pipeline Shutdown*, NEWSWEEK (May 11, 2021), https://www.newsweek.com/darkside-hacker-group-russia-colonial-pipeline-1590352; Press Release, Fed. Bureau of Investigation, FBI Statement on Compromise of Colonial Pipeline Networks (May 10, 2021), https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks.

[8] Patrick De Haan (@GasBuddyGuy), TWITTER (May 13, 2021, 8:08 AM), https://twitter.com/GasBuddyGuy/status/1392813939197726725.

[9] Brett Molina & Nathan Bomey, *Colonial Pipeline Restarted Operations, Owners Say 'it Will Take Several Days' for Supply Chain to Return to Normal*, USA TODAY (May 12, 2021), https://www.usatoday.com/story/money/2021/05/12/gas-shortage-gas-prices-colonial-pipeline-nc-virginia-north-carolina/5052551001/.

[10] Rosa-Aquino & Danner, *supra* note 2.

[11] *Id.*

The Colonial Pipeline hack involved ransomware, a type of malicious software that cyber criminals use to control access to computer systems.[12] In these types of attacks, the hacker usually holds the computer system hostage and demands a ransom be paid for its release.[13] In the event that the ransom is not paid, the ransomware can spread to other systems or data and the hacker can encrypt or delete them all together.[14] Ransomware can be used to target individuals as well as corporate networks. "More than 4,000 ransomware attacks have occurred" everyday since the start of 2016.[15] Cyberattacks on U.S. critical infrastructure, like the pipeline system, could result in millions of dollars in economic damages or drastic harm to the environment, all while putting the welfare and safety of U.S. citizens at risk. The United States has over two million miles of pipelines that supply natural gas, hazardous liquids, and other chemicals to customers around the country.[16] Pipelines are classified as part of the Transportation Systems Sector of U.S. critical infrastructure, over which the Department of Homeland Security and the Department of Transportation share risk management responsibilities.[17]

This Comment will examine the voluntary standards of U.S. pipeline cybersecurity and the private-public partnership. The last four presidential administrations have used this same strategy of voluntary standards and viewed cybersecurity as a private-public partnership.[18] This approach has come up short as evidenced by the Colonial Pipeline attack. This Comment will argue for mandatory cybersecurity standards and show how the Transportation Security Administration

[12] CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY., RANSOMWARE WHAT IT IS AND WHAT TO DO ABOUT IT, https://www.cisa.gov/uscert/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf.
[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] *Critical Infrastructure Sectors*, CYBER AND INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/critical-infrastructure-sectors (last visited Nov. 7, 2021).
[18] Volz, *supra* note 1.

(TSA) can use the Federal Energy Regulatory Commission's (FERC) cybersecurity standards as a framework to help make the U.S. pipeline system cybersecure.

Part II of this Comment will discuss the background and history of critical utility infrastructure and who has responsibility for pipeline cybersecurity. Part III will provide a closer look at the Colonial Pipeline attack. It will touch on who was behind the attack, the failings of the U.S. government, the immediate impact, and future implications. Part IV will talk about the U.S. government's response since the attack. Part V will cover FERC and the various ideas and suggestions from officials and others about what went wrong and what should be done to prevent cyberattacks on critical U.S. infrastructure in the future. Lastly, Part VI will argue for the TSA to adopt FERC's cybersecurity standards and weigh the arguments against making them mandatory for U.S. pipelines.

## II. BACKGROUND OF CRITICAL UTILITY INFRASTRUCTURE IN THE UNITED STATES

Critical infrastructure is "the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety."[19] The critical infrastructure of a country consists of highways, bridges, railways, and utilities that are needed to support daily life.[20] "Transportation, commerce, clean water, and electricity all rely on" critical infrastructure.[21] The United States defines sixteen "critical infrastructure sectors."[22] The sectors are dependent on one another and when one is impacted, the effect is felt across all sectors.[23]

---

[19] *Infrastructure Security*, CYBER AND INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/infrastructure-security (last visited Nov. 7, 2021).
[20] *Critical Infrastructure*, DEP'T. OF HOMELAND SEC., https://www.dhs.gov/science-and-technology/critical-infrastructure (last visited Nov. 7, 2021).
[21] *Id.*
[22] *Critical Infrastructure Sectors*, *supra* note 17.
[23] *Energy Sector*, CYBER AND INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/energy-sector (last visited Nov. 7, 2021).

The stability of the United States and its society are dependent on the nation's critical infrastructure. In 1998, President Clinton issued a directive on protecting the country's critical infrastructure.[24] The aim of the directive was to protect critical infrastructure from attacks that hurt the ability of the federal government, state government, and private sector to protect the safety of the people and stability of the economy.[25] Then, in 2013, President Obama built upon this with another directive that essentially just encouraged public and private organizations to work with one another to make the critical infrastructure that they had control over more secure.[26]

The Energy Sector relies heavily on the pipeline systems housed within the Transportation Systems Sector.[27] The Energy Sector supplies fuel and electricity to businesses and residences necessary for production and comfort.[28] Pipelines are essential to the function of the Energy Sector in order to distribute their products all over the country.[29] The pipeline systems span the entire country "carrying nearly all the nation's natural gas and about 65 percent of hazardous liquids, as well as various chemicals."[30]

The role that pipeline systems play in critical infrastructure is becoming increasingly important as natural gas has emerged as a major part of the United States' electric generation mix.[31] This emergence is due to several reasons: natural gas has a lower carbon impact than other fossil fuels, plants only take two years to build, it is relatively affordable, and there is an abundance of

[24] Mark Weatherford, *The Feds Are Pushing Harder On Infrastructure Security. States and Localities Need to Pay Attention*, GOVERNING (Aug. 10, 2021), https://www.governing.com/security/the-feds-are-pushing-harder-on-infrastructure-security-states-and-localities-need-to-pay-attention.
[25] *Id.*
[26] *Id.*
[27] *Energy Sector*, *supra* note 23.
[28] *Id.*
[29] *Id.*
[30] *Transportation Systems Sector*, CYBER AND INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/transportation-systems-sector (last visited Nov. 7, 2021).
[31] Anmar Frangoul, *Natural Gas: Why it's Important and What You Need to Know*, CNBC (Apr. 25, 2017), https://www.cnbc.com/2017/04/25/natural-gas-why-its-important-and-what-you-need-to-know.html.

it.[32] Natural gas is mainly used for heating and generating electricity within the United States, but it is becoming increasingly popular in industrial and commercial sectors.[33] According to the U.S. Energy Information Administration, natural gas accounted for thirty-four percent of total energy consumption within the United States in 2020.[34] This rise of the importance of natural gas to the fuel mix of the United States "has greatly raised the stakes for pipeline cyber security."[35]

There are currently "a patchwork of piecemeal federal cybersecurity requirements on critical infrastructure that are either narrowly specific to individual sectors, like finance and chemical, or mandated under state or local law, like electricity."[36] There are no overarching cybersecurity requirements for critical infrastructure as a whole and all sectors are overseen by different bodies. Today, the TSA is responsible for the cybersecurity of pipelines that are part of the Transportation Systems Sector.[37] The Aviation and Transportation Security Act created the TSA in 2001 with the mission of guarding against terrorist attacks involving transportation.[38] The TSA is responsible for civil aviation security and other modes of transportation that are run by the Department of Transportation.[39] Congress gave the TSA the responsibility for both the physical and cyber security of pipelines "because they transport fuel, gas and chemicals."[40]

---

[32] *Id.*
[33] *Natural Gas Explained*, U.S. ENERGY INFO. AGENCY, https://www.eia.gov/energyexplained/natural-gas/use-of-natural-gas.php, (last viewed Nov. 7, 2021).
[34] *Id.*
[35] Neil Chatterjee & Richard Glick, *Cyber Security Rules Needed For Pipelines: FERC Commissioners*, CHRON (June 17, 2018), https://www.chron.com/business/energy/article/Cyber-security-rules-needed-for-pipelines-FERC-13002008.php.
[36] Volz, *supra* note 1.
[37] *Pipeline Security Guidelines*, TRANSP. SEC. ADMIN., (2021), https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf.
[38] *Mission*, TRANSP. SEC. ADMIN., https://www.tsa.gov/about/tsa-mission (last view Nov. 7, 2021).
[39] *Pipeline Security Guidelines*, *supra* note 37.
[40] Samantha Schwartz, *TSA Directive Will Add Teeth to Pipeline Security Oversight*, CYBERSECURITY DIVE (May 27, 2021), https://www.cybersecuritydive.com/news/tsa-dhs-cybersecurity-requirements-pipeline-colonial-ransomware/600929/.

Well before the Colonial Pipeline attack, there were signs of "significant weaknesses" in the TSA's handling of pipeline cybersecurity.[41] The TSA had relied heavily on voluntary compliance from the private owners of pipelines.[42] The TSA released voluntary pipeline security guidelines in 2011 and issued a revised version in 2018.[43] After an audit by the Government Accountability Office ("GAO")[44] that was critical of the revised guidelines, the TSA issued a new, and still voluntary, version in April, 2021.[45] The GAO also recommended creating clear guidance for identifying critical facilities because thirty-four of the country's top one-hundred pipelines had not identified any critical facilities and it took the TSA two and a half years to complete this recommendation.[46]

At a congressional hearing in 2019 on protecting U.S. transportation from cyberattacks, the TSA confirmed that it prefers voluntary standards because it allows for "greater flexibility to protect against an evolving threat environment."[47] There is a chance, however, that the TSA prefers this method because it lacks the resources in cybersecurity to create and implement mandatory standards.[48] The Pipeline Security Branch consisted of one full time employee in 2014 and by 2019, that number only increased to five.[49] Given the lack of attention paid to the security

[41] U.S. GOV'T. ACCOUNTABILITY OFF., GAO-19-48, CRITICAL INFRASTRUCTURE PROTECTION 2 (2018), https://www.gao.gov/assets/gao-19-48.pdf.
[42] Brian Naylor, *Beyond Airport, 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.
[43] Sonal Patel, *DHS Issues Pipeline Cybersecurity Directive but Industry Championing FERC Mandatory Standards*, POWER (May 31, 2021), https://www.powermag.com/dhs-issues-pipeline-cybersecurity-directive-but-industry-championing-ferc-mandatory-standards/.
[44] *Critical Infrastructure Protection*, *supra* note 41.
[45] Patel, *supra* note 43.
[46] Shardul Desai & Marissa Serafino, *What TSA's New Cybersecurity Standards Mean For Pipelines*, LAW360 (Aug 17, 2021), https://www.law360.com/articles/1413177.
[47] *Id.*
[48] *Id.*
[49] *Id.*

of pipelines and the voluntariness of their recommendations, it was only a matter of time until the TSA's shortcoming in pipeline cybersecurity would be exposed.

## III. THE COLONIAL PIPELINE ATTACK

What is a cyberattack exactly? "Cyberattacks are unwelcome attempts to steal, expose, alter, disable, or destroy information through" illicit entry of computer systems.[50] Cyberattacks can be associated with terrorism and warfare as well as crime. Most commonly, cyberattackers have criminal and financial motives and try to achieve these goals through stealing money and data or through business disruption.[51] Cybercrime rates increase every year, with "53 percent of cyber attacks result[ing] in damages of $500,000 or more."[52]

"Colonial Pipeline is the largest refined products pipeline in the United States," and it conveys over a hundred million gallons of fuel every day to satisfy the energy needs of the country.[53] On April 29, 2021, hackers gained access to the computer systems of the privately owned operator of the pipeline, Colonial Pipeline Company.[54] The hackers were able to gain entry using a virtual private network account that allows employees to access the company's computer network remotely.[55] The password used for the account was found in a set of leaked passwords on the dark web, meaning that an employee of the pipeline company most likely used the same password on a different platform that was hacked previously.[56]

---

[50] WHAT IS A CYBER ATTACK?, https://www.ibm.com/topics/cyber-attack (last visited Nov. 7, 2021).
[51] *Id.*
[52] WHAT IS A CYBER ATTACK?, https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html (last visited Nov. 7, 2021).
[53] *About Us*, COLONIAL PIPELINE CO., https://www.colpipe.com/about-us (last viewed Nov. 7, 2021).
[54] William Turton & Kartikay Mehrotra, *Hackers Breached Colonial Pipeline Using Compromised Password*, BLOOMBERG (June 4, 2021), https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.
[55] *Id.*
[56] *Id.*

The hacked account did not use multifactor authentication, which means that all the hackers needed was a username and password to access the largest refined oil products pipeline in the country.[57] Once inside, the hackers disrupted the pipeline's operations and the company's CEO made the decision to shut down the pipeline.[58] The hackers then sent a ransom note to the company that demanded nearly five million dollars in Bitcoin.[59] The company paid the ransom the day after learning of the attack due to the severity of the possible consequences if the pipeline remained shut down.[60] Due to the fact that the pipeline supplies nearly half of the eastern United States' gasoline, shortages, price spikes, and buyer panic resulted from the shutdown.[61] The panic reached such a level that the U.S. Consumer Product Safety Commission felt the need to tweet out a warning telling customers "[d]o not fill plastic bags with gasoline."[62] After the ransom was paid, the pipeline was back up and running within a week, which helped to avoid any long term impacts on supply and the price of energy products.[63]

Traditionally, it was thought the only way that the United States' critical infrastructure could be hacked was if another nation was behind it, as they would be the only ones capable of doing so.[64] This thought never really bothered U.S. policymakers as a state-sponsored attack on

---

[57] Sara Morrison, *How a Major Oil Pipeline Got Held For Ransom*, VOX (June 8, 2021), https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices.
[58] WHAT IS A CYBER ATTACK?, *supra* note 50.
[59] *Id.*; For an explanation of Bitcoin see, Kevin Voigt, *What is Bitcoin? BTC Price and How it Works*, NERDWALLET (Mar. 17, 2022), https://www.nerdwallet.com/article/investing/what-is-bitcoin ("Bitcoin is decentralized digital cash that eliminates the need for intermediaries like banks and governments, using instead a peer-to-peer computer network to confirm purchases directly between users."). For a reason why hackers would want to be paid in Bitcoin see, *Why Do Hackers Use Bitcoin? And Other Cybersecurity Questions Answered*, ECPI BLOG, https://www.ecpi.edu/blog/why-do-hackers-use-bitcoin-and-other-cybersecurity-questions-answered ("Hackers like to use bitcoin because of its anonymity. Converting your money to bitcoin, sending, and receiving it doesn't even require the use of a legal name or address. When it comes to a method of acquiring untraceable funds, it's a criminal's dream come true.").
[60] Wilkie, *supra* note 6.
[61] Morrison, *supra* note 57.
[62] US Consumer Product Safety Commission (@USCPSC), TWITTER (May 12, 2021, 10:09 AM) https://twitter.com/USCPSC/status/1392482092823502849.
[63] Morrison, *supra* note 57.
[64] Clare Duffy, *Colonial Pipeline Attack: A 'Wake up Call' About the Threat of Ransomware*, CNN (May 16, 2021), https://www.cnn.com/2021/05/16/tech/colonial-ransomware-darkside-what-to-know/index.html.

U.S. critical infrastructure would be seen as a declaration of war and that no country would dare tempt a U.S. military response.[65] As demonstrated by the Colonial Pipeline hack, this way of thinking is now obsolete. The attack has now been confirmed to have been carried out by a cybercrime group called DarkSide.[66] The group most likely operates from somewhere within Russia or a country close by as most of its online activity is in Russian and it only attacks entities in countries that do not speak Russian.[67] Despite the fact it is known that the group likely operates in Russia, Russian authorities generally leave hacker groups like DarkSide alone as long as their targets are outside of the country.[68]

DarkSide's business model is essentially "ransomware-as-a-service" and helps other criminals in carrying out their hacks.[69] Their signature style of hack usually involves ransomware attacks, where the hackers steal an entity's data, lock their computer systems, and demand payment from the victim to regain access.[70] DarkSide uses a double extortion method, in which the hackers encrypt the data but also take it out of the system and threaten to release it to the public if their demands are not met.[71] This method of extortion makes it even harder for companies to resist DarkSide's ransom request. After the ransom is paid, DarkSide receives a share of the ill-gotten gains.[72] Following the Colonial Pipeline hack, DarkSide issued a statement claiming that they are not politically motivated and wish only to make money, not harm society.[73]

---

[65] *Id.*
[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] Duffy, *supra* note 64.
[70] *Id.*
[71] Sonal Patel, *Colonial Pipeline Ransomware Attack Rattles Power Industry, Renews Vulnerability Concerns*, POWER (May 11, 2021), https://www.powermag.com/colonial-pipeline-ransomware-attack-rattles-power-industry-renews-vulnerability-concerns/.
[72] Duffy, *supra* note 64.
[73] Palmer, *supra* note 7.

The United States should use this attack as an opportunity to improve on their cybersecurity weaknesses. The shortcomings of the TSA were exposed on a grand scale by this cyberattack, yet the negative impact was only a fraction of what it could have been thanks to the hackers being only interested in money and not geopolitics or terrorism. It does not take much imagination to think of the damage that a terror organization could wreak on the economy or society if they had the power to disrupt the nation's pipelines as DarkSide was able to do. The TSA's voluntary guidelines issued after the attack do contain suggestions on access control.[74] The TSA recommends that pipeline operators use "stringent identity and access management practices."[75] Put simply, the TSA did not require multifactor authentication for accounts with access to critical pipeline controls and so Colonial Pipeline Company did not employ this security measure. This made it much easier for the hackers to gain access to their system. As the Federal Energy Regulatory Commission Chairman, Richard Glick, stated, "[t]he cyberattack against the Colonial Pipeline system, which provides nearly half of the fuel supply for the East Coast, is a stark reminder that we must do more to ensure the safety of our nation's energy infrastructure."[76]

## IV. REACTION AFTER THE ATTACK

In July 2021, President Biden issued a new directive that instructed federal agencies to create new voluntary cybersecurity targets for the companies that control critical infrastructure.[77] The directive imposes no new requirements on these operators, but it seeks to develop further voluntary cybersecurity standards that operators can choose whether or not to adhere to.[78] A senior

[74] *Pipeline Security Guidelines*, *supra* note 37.
[75] *Id.*
[76] *Statement from FERC Chairman Richard Glick: Chairman Glick and Commissioner Clements Call for Examination of Mandatory Pipeline Cyber Standards in Wake of Colonial Pipeline Ransomware Incident*, FED. ENERGY REGUL. COMM'N, May 10, 2021, https://www.ferc.gov/news-events/news/statement-ferc-chairman-richard-glick-chairman-glick-and-commissioner-clements.
[77] Volz, *supra* note 1.
[78] *Id.*

administration official was quoted as saying that "[t]he administration is committed to leveraging every authority we have, though limited, and we're also open to new approaches, both voluntary and mandatory."[79] The official also said that the reason they are staying with a voluntary approach is that they "want to do this in full partnership."[80]

Historically, conservatives have been against requiring companies to report a cybersecurity breach, however, there has been renewed interest in creating such requirements from both sides of the aisle since the Colonial Pipeline attack.[81] Lawmakers expect pushback from business interest groups about such requirements, but members of Congress have recently began speaking more forcefully on the issue.[82] Senator Sheldon Whitehouse (D-R.I.), was quoted as saying that "[w]e should no longer tolerate this voluntary regime with big companies who know that their infrastructure is critical and who fail."[83] He went on to say that the Colonial Pipeline hack showed that the voluntary approach to cybersecurity was inadequate.[84] In another sign that the attack has spurred action in Congress, a group of bipartisan lawmakers, including members of the Senate Intelligence Committee, introduced legislation that would require those responsible for critical infrastructure to report cyberattack attempts.[85] This piece of legislation is called the Cyber Incident Notification Act of 2021 and has the backing of Senator Marco Rubio.[86]

Following the attack, on May 28, 2021, the TSA the issued their own directive specifically targeted at enhancing pipeline cybersecurity.[87] This directive included three mandatory

[79] *Id.*
[80] *Id.*
[81] *Id.*
[82] Volz, *supra* note 1.
[83] *Id.*
[84] *Id.*
[85] Steve Reardon, *Bipartisan Bill to Require Certain Companies to Disclose Cyber Attacks*, LAW.COM (Aug. 18, 2021), https://www.law.com/dailybusinessreview/2021/08/18/bipartisan-bill-to-require-certain-companies-to-disclose-cyber-attacks/.
[86] *Id.*
[87] Desai & Serafino, *supra* note 46.

requirements for companies that operate pipelines: (1) all cyberattacks must be reported to the Cybersecurity and Infrastructure Security Agency (CISA) within twelve hours; (2) a coordinator must be designated who the TSA and CISA can get in touch with 24/7; and (3) an assessment of the pipeline's weaknesses must be conducted and given to the TSA and CISA.[88] Following this directive, more mandatory cybersecurity standards were put in place by the TSA on July 20, 2021.[89] This "reversed two decades of pipeline cybersecurity policies" in which the TSA took a voluntary approach to cybersecurity standards.[90] These new mandatory standards require pipeline operators to "immediately implement mitigation measures to protect against cyberattacks, to develop a cybersecurity contingency and recovery plan, and to conduct a cybersecurity architecture design review."[91] If these new measures are not followed, the pipeline operator could be fined up to $11,904 a day per violation.[92]

This new mandate has already come under fire because some of its requirements are seen as too much of a burden on pipeline operators.[93] The entirety of the directive was not made public, but Tennessee Senator Marsha Blackburn has said that she is hearing concerns from pipeline companies about the feasibility of the new rules.[94] "Companies might have to upgrade thousands of pieces of equipment that they can't even get due to supply chain shortages," Blackburn said.[95] The Senator went on to suggest that the TSA should make their cybersecurity mandates more

[88] *Id.*; s*ee About CISA*, CYBER AND INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/about-cisa (last visited Nov. 7, 2021) (explaining CISA is a federal agency under the Department of Homeland Security that defends against cyberattacks).
[89] *Id.*
[90] *Id.*
[91] *Id.*
[92] *Id.*
[93] Gerson Freitas Jr., *Sen. Blackburn Says Pipe Operators Concerned About Cyber Rules*, BLOOMBERG LAW (July 27, 2021), https://news.bloomberglaw.com/privacy-and-data-security/sen-blackburn-says-pipe-operators-concerned-about-cyber-rules.
[94] *Id.*
[95] *Id.*

attainable and that they should work more closely with the private pipeline companies in order to achieve this.[96]

The new cybersecurity mandate has also come under fire because the TSA skipped the usual rulemaking process, which would have permitted stakeholder input through notice and comment.[97] Members of the U.S. Senate Committee on Commerce, Science, and Transportation objected to the unusual manner in which mandate was handed down.[98] In response to the mandate, Senators on the Committee issued a statement saying that the benefit of the normal "public notice and comment through the rulemaking process" helps the TSA to "avoid any unintended consquences that disrupt existing effective cybersecurity practices or transportation operations."[99] The TSA is allowed to issue directives like this only if it determines that it "must be issued immediately in order to protect transportation security."[100] Members of the Committee went on to say that the use of emergency authority was inappropriate in this scenario because of a lack of an immediate threat and they would like to see the TSA to go back to the longer rulemaking process.[101] Senators also criticized the TSA for not first sharing the directives with Congress before they were issued, as is the norm for TSA rulemaking.[102] The new directive might be difficult for the TSA to defend considering it took them over two years to even provide guidance on how to identify critical facilities and TSA's history of being understaffed and lacking knowledge of cybersecurity.[103] Simply put, the new directive is coming across to those in the

[96] *Id.*
[97] Desai & Serafino, *supra* note 46.
[98] Mariam Baksh, *TSA Considers Rulemaking Process for Cybersecurity in Transportation Sector*, NEXTGOV (Nov. 2, 2021), https://www.nextgov.com/cybersecurity/2021/11/tsa-considers-rulemaking-process-cybersecurity-transportation-sector/186580/.
[99] *Id.*
[100] 49 U.S.C. § 114(l)(2)(A).
[101] Baksh, *supra* note 98.
[102] *Id.*
[103] Desai & Serafino, *supra* note 46.

industry as a hasty and poorly thought out response by the TSA to try to make up for their past shortcomings in the pipeline cybersecurity.[104]

## V. MAKING PIPELINES MORE CYBERSECURE

The Energy Policy Act of 2005 made the Federal Energy Regulatory Commission ("FERC") responsible for the oversight of the bulk power system, which is essentially the power grid of the country.[105] This oversight responsibility includes with it the power to implement mandatory cybersecurity standards for operators of the power grid.[106] In coordination with the North American Electric Reliability Corporation ("NERC"),[107] FERC has put in place mandatory cybersecurity rules that have kept the power grid cybersecure for over a decade.[108] Despite the success of FERC in keeping the bulk power system of the United States safe from cyberattacks with their mandatory standards, there are no comparable mandatory rules for the over two million miles of pipeline systems that are vital to the country.[109] Like FERC, TSA has the power to create and enforce mandatory cybersecurity standards to protect pipeline infrastructure, but instead has historically only relied on the voluntary approach.[110]

The number of bad cyber actors and their level of sophistication is only increasing.[111] Encouraging pipeline operators to adopt safe cybersecurity practices is an insufficient response to the threat that these cybercriminals pose.[112] Jim Robb, the President and CEO of NERC,

---

[104] Freitas Jr., *supra* note 93.
[105] *Cyber and Grid Security*, FED. ENERGY REGUL. COMM'N (Dec. 17, 2021), https://www.ferc.gov/industries-data/electric/industry-activities/cyber-and-grid-security.
[106] *Id.*
[107] *See About NERC*, N. AM. ELEC. RELIABILITY CORP., https://www.nerc.com/AboutNERC/Pages/default.aspx ("The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.").
[108] *Cyber and Grid Security*, *supra* note 105.
[109] *Statement from FERC Chairman Richard Glick*, *supra* note 76.
[110] Patel, *supra* note 43.
[111] *Id.*
[112] *Id.*

recognizes the inadequacy of pipeline cybersecurity and has insisted that the gas pipeline industry adopt standards that are like NERC's reliability standards.[113] Mr. Robb implored "policymakers to refocus on ensuring that gas infrastructure is as secure as the grid it supplies."[114] Congress has thus far resisted calls to transfer the responsibility of pipeline cybersecurity to another body, perhaps seeing those calls as a calculated move by NERC in order to gain more power.[115]

The Industrial Energy Consumers of America ("IECA") is one non-profit interest group advocating for FERC to be given authority over the cyber and physical security of pipelines.[116] The group's position is that FERC is much better equipped to handle this responsibility because it "meets at the intersection of natural gas and electricity markets that are dependent upon one another," according to IECA President and CEO Paul Cicio.[117] FERC already has some authority over aspects of the pipeline system, like the ability to set their rates or issue certificates for the construction of new pipelines.[118] Proponents of giving the responsibility for pipeline security to FERC see it as a simple and smart switch that would allow the TSA to focus on "the security of 851 million aviation passengers per year, 138,000 miles of railroad track, and four million miles of highway."[119]

To maintain cybersecurity for the power grid, FERC employs its Critical Infrastructure Protection ("CIP") reliability standards.[120] The CIP standards mandate that the operators of the

[113] *Id.*
[114] *Id.*
[115] Patel, *supra* note 43.
[116] *Id.*
[117] *Id.*
[118] *Id.*
[119] *Id.*
[120] Will Daugherty & Susan Ross, *Incentivizing Public Utilities to Enhance Cybersecurity: FERC's Proposed Legislation*, NORTON ROSE FULBRIGHT: DATA PROTECTION REPORT (Feb. 11, 2021), https://www.dataprotectionreport.com/2021/02/incentivizing-public-utilities-to-enhance-cybersecurity-fercs-proposed-regulation/.

power grid "comply with specific requirements to safeguard critical cyber assets."[121] Although they must comply with these standards, FERC's policy is results-based, meaning they do not specify what method must be used to comply, only that the standards must be complied with.[122] The entity is then left to decide how best to meet these requirements in a way that works for their individualized company.[123] This is materially different from TSA's mere voluntary suggestions of what standards to use. If the pipelines choose not to follow the suggestions, there is no punishment. FERC on the other hand, will fine companies that do not meet the CIP standards.[124]

In February 2021, FERC published new regulations that would give financial incentives to power grid operators that put in place increased cybersecurity measures that went further than those required by the CIP standards.[125] This is not mandatory, but FERC is using this program to incentivize the operators to go above and beyond the minimum standards. To get the financial reward, the new measures need to "materially enhance the cybersecurity posture of the bulk-power system by enhancing the applicants' cybersecurity posture substantially above levels required by CIP Reliability Standards."[126] FERC recognizes that utilities are faced with ever-evolving and sophisticated cybersecurity challenges and that the standards will not be able to be updated fast enough to keep up.[127] That is why it is imperative for the government, through FERC, to have a minimum set of standards and also have rules that incentivize utility companies to push past base levels of requirements. This incentive program also encourages cybersecurity improvements to be

[121] *Id.*
[122] *Id.*
[123] *Id.*
[124] *Id.*
[125] Will Daugherty & Susan Ross, *Incentivizing Public Utilities to Enhance Cybersecurity: FERC's Proposed Legislation*, NORTON ROSE FULBRIGHT: DATA PROTECTION REPORT (Feb. 11, 2021), https://www.dataprotectionreport.com/2021/02/incentivizing-public-utilities-to-enhance-cybersecurity-fercs-proposed-regulation/.
[126] *Id.*
[127] *Id.*

made quickly because once a specific improvement is made mandatory, the utilities without it are no longer eligible for the financial incentive.[128]

The mandatory minimum standards that FERC uses are created by standards drafting teams, consisting of industry volunteers who, with the support of NERC staff, create the rules using results-based principles.[129] The standards use a defense-in-depth strategy in which each part of the standard plays a role in preventing harm.[130] This strategy is created when "there is an appropriate portfolio of performance-, risk-, and competency-based mandatory reliability requirements that complement and reinforce each other."[131] Every requirement should pinpoint a specific and quantifiable expected outcome, along the lines of: "a) a stated level of reliability performance, b) a reduction in a specified reliability risk (prevention), or c) a necessary competency,"[132] as illustrated here:

> a) Performance-Based—defines a particular reliability objective or outcome to be achieved. In its simplest form, a results-based requirement has four components: who, under what conditions (if any), shall perform what action, to achieve what particular result or outcome?
> b) Risk-Based—preventive requirements to reduce the risks of failure to acceptable tolerance levels. A risk-based reliability requirement should be framed as: who, under what conditions (if any), shall perform what action, to achieve what particular result or outcome that reduces a stated risk to the reliability of the bulk power system?
> c) Competency-Based—defines a minimum set of capabilities an entity needs to have to demonstrate it is able to perform its designated reliability functions. A competency-based reliability requirement should be framed as: who, under what conditions (if any), shall have what capability, to achieve what particular result or outcome to perform an action to achieve a result or outcome or to reduce a risk to the reliability of the bulk power system?[133]

---

[128] *Id.*
[129] *Results Based Standards*, N. AM. ELEC. RELIABILITY CORP., https://www.nerc.com/pa/Stand/Pages/ResultsBasedStandards.aspx.
[130] *Id.*
[131] *Id.*
[132] *Id.*
[133] *Id.*

Congress should give the power over pipeline security to a government entity "that fully comprehends the nation's energy sector and has sufficient resources to address the growing cyber security threat to gas pipelines," said former FERC Chairman, Neil Chatterjee.[134] The Department of Energy (DOE)—and FERC as an independent agency with DOE—have vast amounts of experience with energy security.[135] Those are the agencies within the federal government that should be responsible for pipeline security, not TSA. But just because it would be a good idea does not mean Congress will pass legislation making it so. Congress has thus far resisted calls from major industry experts, like Mr. Chatterjee, to do so.[136] Whether the responsibility for pipeline cybersecurity is shifted to another government agency or not, the U.S. must establish mandatory pipeline cybersecurity standards like those used by the electric power sector. Mandatory cybersecurity standards are vital to protect the U.S. critical infrastructure pipeline system that the nation depends on.

## VI. TSA SHOULD UTILIZE THE PROVEN FERC CYBERSECURITY FRAMEWORK

Cybercriminals and state actors are increasingly launching cyberattacks on critical infrastructure of the U.S. and other nations around the world.[137] A survey of employees at companies responsible for critical infrastructure in the U.S. showed that ninety percent of those surveyed had at least one security incident in the past year.[138] An even scarier stat is that in the last twelve months, fifty-six percent of energy utilities reported a cyberattack.[139] Although this

[134] Chatterjee & Glick, *supra* note 35.
[135] *Id.*
[136] *Id.*
[137] Adam Weinberg, *Analysis of Top 11 Cyber Attacks on Critical Infrastructure*, FIRSTPOINT (June 2, 2021), *https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure/* (analyzing the top eleven cyberattacks on critical infrastructure around the world).
[138] *Id.*
[139] *Id.*

may sound frightening, FERC has the necessary policies in place to prevent these attacks on energy utilities from becoming major catastrophes.

The mandatory standards for operators that FERC enacted protect the electric sector from cyberattacks. Despite fifty-six percent of energy utilities reporting a cyber incident last year, FERC has been successful in preventing any major cyberattack from disrupting operations in the bulk power system since it took over responsibility in 2005.[140] There are no such similar standards in place to protect natural gas pipelines.[141] In order to shield the United States from the dangers of cyberattacks on pipelines, TSA should use FERC's CIP standards and incentive program as a base framework for mandatory cybersecurity standards for the pipeline system.

The Biden administration and other members of Congress have shown interest in improving the cybersecurity of critical infrastructure in the United States and mandatory regulations could be implemented in the near future.[142] Power "grids require the security of both information technology (IT) and operational technology (OT) systems."[143] This is the same for pipelines and so "the FERC CIP cybersecurity standards provide a framework" of how mandatory cybersecurity requirements for the pipeline system should look.[144] Most of the TSA's mandates only apply to the top one hundred most critical pipelines even though there are more than 3,000 pipeline operators throughout the United States.[145] If the TSA were to adopt an incentive program, on top of mandatory minimum standards for the most critical pipelines, this could help to

[140] *Cyber and Grid Security*, *supra* note 105.
[141] *Id.*
[142] Desai & Serafino, *supra* note 46.
[143] *Id.*; *see Operational Technology (OT) – Definitions and Differences with IT*, I-SCOOP, https://www.i-scoop.eu/industry-4-0/operational-technology-ot/ (explaining "[o]perational technology or OT is a category of computing and communication systems to manage, monitor and control industrial operations with a focus on the physical devices and processes they use. Operational technology, monitors and manages industrial process assets and manufacturing/industrial equipment").
[144] *Id.*
[145] Patel, *supra* note 43.

encourage all of the pipelines to improve their cybersecurity facilities, not just the largest operators.

There will undoubtedly be differences in the cybersecurity needs between the Energy and Transportation System sectors. The cybersecurity of pipelines is "uniquely challenging."[146] Pipelines travel long distances, which means that they need their IT and OT systems to allow for communication "across vast geographic space through the use of long-distance telecommunication infrastructure."[147] Because of this, the cybersecurity of pipeline systems needs to have IT and OT security as well as cyber policies concerned with the telecommunication infrastructure.[148] All of this must be taken into account in order to have cybersecurity program that protects the pipeline from cyberattacks, identifies possible weaknesses, and lets the operators be prepared for new threat developments.[149]

Creating standards using FERC's results-based approach and implementing an incentive program to go above and beyond the base requirements is a necessary first step to prevent another Colonial Pipeline attack. FERC has been successful in preventing a major attack like the Colonial Pipeline hack from happening to the electric sector. Their approach is flexible because they realize that utilities face complex and changing threats. This is why FERC uses a results-based approach that focuses on the results rather than the methods to achieve them. The TSA should adopt a similar CIP results-based set of minimum standards with the addition of an incentive program to cope with the changing cybersecurity landscape in order to bring maximum protection to the pipeline system in the United States.

A. *Addressing the Counter Arguments*

[146] Desai & Serafino, *supra* note 46.
[147] *Id*.
[148] *Id.*
[149] *Id.*

One of the main reasons why some pipeline operators do not want mandatory cybersecurity standards is the idea that they become obsolete too quickly.[150] Executives in the industry believe that cyber threats are too hard to pinpoint, and this calls for an approach that allows operators to handle them without adhering to specific rules that could slow them down.[151] Thomas Fanning, CEO of Southern Company, a utility company based out of Atlanta, believes that new mandates will just impede companies' attempts to improve their cybersecurity.[152] "Just being compliant [with regulations] will fail to achieve the real-time efforts necessary to beat our adversaries," Mr. Fanning said.[153]

Apart from concerns about new mandates getting in the way, the "industry has also warned that proposals to shift pipeline security oversight outside of the TSA . . . could create more problems than it solves if it subjects pipelines to overlapping standards."[154] An industry official was quoted as saying "[w]hat would not be helpful and what we want to avoid no matter what is multiple agencies with overlapping or conflicting authorities."[155] A separate issue brought up by those opposed to mandatory cybersecurity standards for pipelines, is that the investment costs in complying will have to be passed on to the consumer.[156] Pipeline operators will be in a hurry to recover the money they spend on improving their cybersecurity and this may cause them to increase rates.[157] This will increasingly put utilities and government agencies "in the unenviable

---

[150] Chris Knight, *US Pipeline Hack Revives Cybersecurity Focus: Update*, ARGUS MEDIA (May 10, 2021), https://www.argusmedia.com/en/news/2213654-us-pipeline-hack-revives-cybersecurity-focus-update.
[151] *Id.*
[152] Dustin Volz & David Uberti, *Biden Says Cybersecurity Is the 'Core National Security Challenge' at CEO Summit*, WALL ST. J. (Aug. 25, 2021), https://www.wsj.com/articles/biden-to-hold-cybersecurity-summit-with-tech-giants-top-banks-energy-firms-11629882002.
[153] *Id.*
[154] Knight, *supra* note 150.
[155] *Id.*
[156] Mark Weatherford, *The Feds Are Pushing Harder On Infrastructure Security. States and Localities Need to Pay Attention*, GOVERNING (Aug. 10, 2021), https://www.governing.com/security/the-feds-are-pushing-harder-on-infrastructure-security-states-and-localities-need-to-pay-attention.
[157] *Id.*

position of deciding how to defend critical infrastructure businesses trying to meet federal cybersecurity regulations through increased investment while at the same time limiting the costs being passed on to ratepayers."[158]

B. *Responses and why it Might Make Sense for TSA to Keep Control*

There is no doubt that increasing the cybersecurity of pipeline operators will lead to increased costs to consumers. "However, one successful attack could shut down tens of thousands of manufacturing facilities and cost tens of millions of dollars per day for each facility. The economic harm could be staggering," according to IECA President and CEO Mr. Cicio.[159] All one needs to do is look at the impact of the Colonial Pipeline attack to see just how quickly an attack on critical infrastructure can negatively impact society. Panic-buying, gas prices surging, and flight disruptions all happened in very short order following the attack. The Colonial Pipeline attack was carried out by a criminal group looking for money. If it were undertaken by a different actor with the intention of causing harm to the United States and its citizens, the results could have much worse. A rise in consumer rates is well worth the protection that increased cybersecurity measures will give to the people of the United States.

Next is the argument that mandatory cybersecurity standards will become obsolete too quickly and get in the way of pipeline operators making changes in real time to meet the needs of the ever-changing cybersecurity threat landscape. The response to this is simple, the public-private partnership strategy of voluntary standards has failed. The United States' critical infrastructure has been hacked and it caused the largest pipeline on the East Coast to completely shut down. Critics say mandatory standards will impede progress, yet there was nothing in place to impede DarkSide as they took control of Colonial Pipeline's computer systems and held them for ransom.

[158] *Id.*
[159] Patel, *supra* note 43.

If TSA employs mandatory standards similar to FERC's results-based approach, the pipeline operators will be free to expand their company's cybersecurity in any way that they see fit, as long as TSA sees the cybersecurity results mandated. This flexible approach will remove the impediments that some executives are concerned about.

Data from IBM shows that ransomware attacks were the most common threat to organizations that use operational technology in 2020.[160] The sectors looked at for this study include manufacturing, oil and gas, transportation, utilities, construction, and mining, where ransomware attacks accounted for thirty percent of all attacks.[161] This all suggests that cybercriminals and other bad cyber actors may be specifically targeting entities that use OT networks because of the heavy costs associated with shutting down operations and the wider impact it may have.[162] Given this data, and the argument that assigning pipeline cybersecurity to another agency could cause confusing overlap, it might be wise for TSA to keep control. This would prevent the confusion and overlap that some industry leaders fear would result if another agency took control. By TSA retaining responsibility, it gives them the chance to develop their own personalized standards (after applying FERC-like baseline standards) that would allow them to focus on unique threats to the pipeline system due to the way they use OT that are not faced by other critical infrastructure sectors.

## VII. CONCLUSION

When critical infrastructure fails or is disrupted, the impact on society can be damaging economically, but it can also threaten the physical well-being of citizens. A recent example of this

[160] Camille Singleton & Anna Seitz, *Attacks on Operational Technology From IBM X-Force and Dragos Data*, SECURITY INTELLIGENCE (July 7, 2021), https://securityintelligence.com/posts/attacks-operational-technology-ibm-dragos-data/.
[161] *Id.*
[162] *Id.*

was in February 2021 when winter storms caused a major power crisis in Texas.[163] The storms caused 4.5 million homes and businesses to lose power, heat, and water during a record cold spell.[164] By the time services were restored, seven hundred people had died as a result of the power crisis.[165] This remarkable incident was the result of mother nature and not an actor intent on causing harm.

If a terrorist group or enemy state can disrupt the United States' critical infrastructure through cyberattacks, the impact could be much worse than that seen in Texas. As the United States continues to lessen its physical presence in the Middle East, it is necessary to reorient national security priorities around new strategic threats.[166] China and Russia's efforts to destabilize Western society and alliances should top that list.[167] One weapon in their arsenal will be cyberattacks on U.S. critical infrastructure through hacks of their own and cybercrime groups located within their borders.

FERC's CIP standards and the creation of new regulations from a results-based creation process can form a foundation for TSA and pipeline operators. The old public-private partnership method of voluntary standards is inadequate as shown by the Colonial Pipeline attack. Despite the possibility of an increase in costs to consumers, mandatory standards are now necessary to prevent an even greater cost to society that would result from a large scale cyberattack on the U.S. critical infrastructure. Congress does not seem motivated to shift the responsibility for pipeline cybersecurity to FERC or any other agency. This may end up being a wise choice if it allows TSA to develop personalized standards, on top of baseline mandatory standards, that are needed to face

[163] Weinberg, *supra* note 137.
[164] *Id.*
[165] Lewis Milford & Shelley Robbins, *Texas Power Outage Deaths: Is Cruelty and Neglect Our New Energy Policy?*, THE HILL (June 28, 2021), https://thehill.com/changing-america/opinion/560540-texas-power-outage-deaths-is-cruelty-and-neglect-our-new-energy.
[166] Volz & Uberti, *supra* note 152.
[167] *Id.*

the cybersecurity challenges specific to pipelines. With the growing importance of natural gas and the increased sophistication of America's enemies, the top item on President Biden's agenda should be securing our critical infrastructure from cyber and physical threats. FERC has already done this with the Energy Sector, and it is time for the TSA to learn from FERC's success and use their framework to secure the Transportation Systems sector and its pipelines.