Pipeline Cybersecurity: Federal Programs

September 9, 2021

Congressional Research Service
https://crsreports.congress.gov
R46903

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R46903

September 9, 2021

Paul W. Parfomak
Specialist in Energy Policy

Chris Jaikaran
Analyst in Cybersecurity Policy

Pipeline Cybersecurity: Federal Programs

The vast U.S. network of natural gas, crude oil, and refined product pipelines is integral to U.S. energy supply and also has vital links to other critical infrastructure such as power plants and airports. This network is vulnerable to cyberattacks. Pipeline companies employ technologies which enable them to achieve business and operational efficiencies, but these technologies are susceptible to cybersecurity risks—and these risks have been growing. The May 2021 ransomware attack against the Colonial Pipeline, which disrupted gasoline supplies throughout the East Coast, highlighted this risk and increased concern in Congress about federal oversight of pipeline cybersecurity. Several bills in the 117th Congress would affect federal pipeline cybersecurity programs, including the Pipeline Security Act (H.R. 3243), the Pipeline and LNG Facility Cybersecurity Preparedness Act (H.R. 3078), and the Promoting Interagency Coordination for Review of Natural Gas Pipelines Act (H.R. 1616). In addition, the Colonial Pipeline incident has led to changes in the federal agency oversight of pipeline cybersecurity under existing statutory authorities.

Pipelines face varied cybersecurity risks. Pipelines rely on information technology (IT), such as laptops, and operational technology (OT), such as pipeline control systems. Using both types of systems creates challenges for cybersecurity. Attacks against IT can compromise the data and business systems of a company. Attacks against OT can cause physical disruptions that increase the probability of pipeline failure and environmental damage. Some attacks to IT (e.g., ransomware) can have an effect on OT as well, if they spread to those systems or the company opts to shut down its OT to prevent further damage.

Two agencies within the Department of Homeland Security have primary responsibility for pipeline cybersecurity: the Transportation Security Administration (TSA) and the Cybersecurity and Infrastructure Security Agency (CISA). TSA has had regulatory authority for security over all transportation—including pipelines—for two decades. For most of this time, TSA relied on voluntary pipeline cybersecurity guidance and best practices. The agency recently imposed mandatory requirements for pipeline cybersecurity after the Colonial Pipeline attack, when it issued two cybersecurity directives. CISA has more extensive cybersecurity capabilities and provides technical expertise to assist both TSA and industry partners in improving cybersecurity. CISA has conducted cyber risk assessments of pipeline operators and has received cybersecurity incident reports from companies pursuant to TSA's pipeline cybersecurity directives. Other federal entities also are involved with pipeline cybersecurity. They include the Department of Transportation's Pipeline and Hazardous Materials Safety Administration, which is the nation's pipeline safety regulator and partners with TSA on security issues, and the Department of Energy's (DOE's) Cybersecurity, Energy Security, and Emergency Response office, which is congressionally mandated to research cybersecurity risks and coordinate federal response to energy sector cyber incidents.

The Government Accountability Office, federal agencies, and industry stakeholders have raised several specific pipeline cybersecurity issues of ongoing interest to Congress. They include the following:

- **Resources.** TSA resources devoted to pipelines (and cybersecurity thereof) have been small relative to its other priorities (e.g., aviation). TSA officials have testified that the agency will increase staffing in fiscal years 2021 and 2022, but it is uncertain whether the increases will be sufficient to manage cyber risk.
- **Standards.** With the issuance of TSA's directives, questions around cybersecurity standards have arisen. TSA is requiring process standards (e.g., having a process to report incidents) rather than design standards (e.g., prescribing a technical specification for user access controls). The sufficiency of this approach is under debate.
- **Agency Roles.** Whether other federal agencies should have responsibility for pipeline cybersecurity has been under discussion. For example, some have argued for DOE to expand further into pipeline cybersecurity or for the Federal Energy Regulatory Commission to regulate pipeline operators.
- **Threat Information.** The quality, quantity, and timeliness of cybersecurity risk information originating with the government and being shared with the private sector continues to be an area of focus.

In addition to these specific issues, Congress may want to assess how the various elements of U.S. pipeline cybersecurity and critical infrastructure security will fit together most effectively in the nation's overall strategy to protect critical pipelines. Pipeline security necessarily involves various groups: federal agencies, pipeline associations, large and small pipeline operators, and the broader industrial cybersecurity community. Reviewing how these groups work together to achieve common goals could be an overarching challenge for Congress.

Contents

Contacts

Introduction

The U.S. energy pipeline network is composed of approximately 3 million miles of pipeline transporting natural gas, crude oil, refined products, and other hazardous liquids.[1] This vast pipeline network is vital to the economy and integral to the nation's energy supply, with links to power plants, refineries, airports, and other critical infrastructure. Although pipelines are regarded as a relatively safe means of transporting materials, they have the potential to cause public injury and environmental harm. Both because of their economic importance and the physical risks they may pose, pipeline systems have drawn attention as targets for terrorism or other malicious activity. Physical attacks on pipelines were historically a priority, but the sophisticated computer systems used to administer and operate pipelines increasingly have become a target of cyberattacks. The May 8, 2021, ransomware attack on the Colonial Pipeline Company, which disrupted gasoline supplies throughout the East Coast, was the most significant attack on a U.S. pipeline computer system. However, pipeline cyberattacks have been occurring for at least a decade.

The Colonial Pipeline incident and previous pipeline cyberattacks have elevated concern in Congress about the cybersecurity of the nation's energy pipelines and federal programs to protect them. A July 13, 2021, report from the House Committee on Homeland Security stated, "as illustrated by the May 2021 Colonial Pipeline attack, the need for the Federal government to raise the bar on cybersecurity among pipeline operators is particularly acute."[2] Several bills in the 117th Congress would affect federal pipeline cybersecurity programs, including the Pipeline Security Act (H.R. 3243), the Pipeline and LNG Facility Cybersecurity Preparedness Act (H.R. 3078), and the Promoting Interagency Coordination for Review of Natural Gas Pipelines Act (H.R. 1616). In addition, the Colonial Pipeline incident has already led to significant changes in the federal oversight of pipeline cybersecurity under existing statutory authorities.

This report discusses cybersecurity risks to natural gas, oil, and refined products pipelines, including to control systems and information technology, as well as ransomware. It summarizes the history of major pipeline cybersecurity warnings and cyberattacks in the United States over the last 15 years. It examines the federal role in protecting U.S. pipelines from cyber threats, including the agencies involved and their pipeline cybersecurity activities. It discusses the federal response to the Colonial Pipeline cyberattack. The report concludes with an overview of selected issues for Congress, including legislative proposals to change federal pipeline security programs.

Pipeline Cybersecurity Risks

Pipeline companies simultaneously operate two different types of technology systems—information technology (IT) and operational technology (OT). Both types of systems create challenges for cybersecurity. IT systems are common across many consumer and business products. IT includes the laptops, software, and networking equipment used for productivity and communications. OT enables cyber-physical linkages which allow dispersed equipment to be centrally monitored and controlled. OT includes industrial control systems (ICS) such as supervisory control and data acquisition (SCADA) systems, distributed control systems, and programmable logic controllers. IT and OT both may be enabled by Internet of Things (IoT)

[1] Pipeline and Hazardous Materials Safety Administration (PHMSA), "Annual Report Mileage Summary Statistics," online tables, May 3, 2021, https://www.phmsa.dot.gov/data-and-statistics/pipeline/annual-report-mileage-summary-statistics.

[2] U.S. Congress, House Homeland Security Committee, *Pipeline Security Act*, 117th Cong., 1st sess., July 13, 2021, H.Rept. 117-85, p. 3.

devices, such as a smart card reader to unlock a door, or a thermometer to maintain proper temperature at a fuel processing facility. IT and OT systems also may share connections, such as an OT system that reports usage (e.g., pipeline shipments) to an IT system that facilitates customer scheduling and billing. The complexity of simultaneously operating both types of systems can create novel opportunities for malicious actors to gain access and manipulate systems.

Industrial Control Systems (ICS) Risks

ICS are a type of OT used to monitor and control many aspects of network operation for railways, power grids, water and sewer systems—and pipeline networks. One category of ICS widely used in pipelines networks—SCADA systems—collects data (e.g., line pressure) in real time from sensors throughout a network and displays those data to human operators in remote network control rooms. These operators can then send computerized commands from SCADA workstations to control geographically dispersed equipment such as pipeline valves, pumps, meters, and many other network components. The SCADA system provides continuous feedback about conditions throughout the pipeline network and generates safety alarms when operating conditions fall outside prescribed levels.[3] ICS communications may employ dedicated telephone landlines, wireless communications (satellite, microwave, and radio), cellular telephone service, Wi-Fi, and the internet. As SCADA technology has matured, system control has become more intelligent and more automated, requiring less human intervention.

Historically, pipeline SCADA systems employed highly customized proprietary software and were physically isolated from external communications and computer networks. Because many of these systems were largely unique to a specific system operator, malicious actors outside the company faced challenges when trying to access and disrupt a SCADA system. But these unique systems were expensive to design, build, and maintain. Due to advancements in computer technology and the development and adoption of advanced communications and internet-based control system applications, SCADA systems have become more standardized and vulnerable to outside intrusion and manipulation.[4] Specific SCADA security weaknesses include the adoption of standardized control system technologies (some with known vulnerabilities), increased connection to external networks, insecure communication connections, and the public availability of sensitive information about control systems and infrastructure.[5]

Once accessible to a knowledgeable attacker, a SCADA system can be exploited in a number of specific ways to carry out a cyberattack:

- issuing unauthorized commands to control equipment;
- sending false information to a control-system operator to initiate inappropriate action;

[3] National Transportation Safety Board, *Supervisory Control and Data Acquisition (SCADA) in Liquid Pipelines*, NTSB/SS-05/02, November 29, 2005, pp. 1-2.

[4] Tobias Walk, "Cyber-Attack Protection for Pipeline SCADA Systems," *Pipelines International Digest*, January 2012, p. 6; Rose Tsang, Cyberthreats, "Vulnerabilities and Attacks on SCADA Networks," working paper, University of California, Goldman School of Public Policy, 2009, p. 2, http://gspp.berkeley.edu/iths/Tsang_SCADA%20Attacks.pdf.

[5] General Accounting Office, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*, GAO-04-354, 2004, pp. 12-13; Eric Byres, "Next Generation Cyber Attacks Target Oil and Gas SCADA," *Pipeline & Gas Journal*, February 2012; Robert O'Harrow Jr., "Cyber Search Engine Exposes Vulnerabilities," *Washington Post*, June 3, 2012. The General Accounting Office subsequently was renamed the Government Accountability Office.

- disrupting control system operation by delaying or blocking the flow of information through the control network;
- making unauthorized changes to control system software to modify alarm thresholds or other configuration settings; and
- rendering resources unavailable by propagating malicious software (e.g., a virus, worm, Trojan horse) through the control network.[6]

In 2014, the Department of Homeland Security (DHS) released information on a project which demonstrated these vulnerabilities.[7] "Project Aurora" was conducted in 2007 by Idaho National Laboratory as a proof-of-concept cyberattack with physical consequences. In this attack, researchers exploited a system vulnerability to gain access to the ICS of a power generator. They proceeded to send commands to the generator to rapidly increase its revolutions, then quickly reverse them, and then repeat that cycle. Concurrently, researchers directed the ICS system to report to the monitoring system that the generator was operating normally. Video of the experiment shows the generator struggle under the malicious command sequence and ultimately fail.

Depending upon the configuration of a particular pipeline system, cyberattacks on ICS potentially could disrupt service, damage equipment, or even cause a hazardous release of pipeline contents. While no pipeline releases due to a cyberattack have been reported publicly in the United States, such an attack reportedly was used in 2008 to cause an explosion of the Baku-Tbilisi-Ceyhan oil pipeline in Turkey.[8]

Information Technology Risks and Ransomware

Ransomware is a particular form of malicious software (malware) which seeks to deny users access to data and IT systems by encrypting the files and systems—thus locking out users. Perpetrators usually extort victims for payment, typically in cryptocurrency, to decrypt the system. Recently, such attacks have been coupled with data breaches in which perpetrators also steal data from their ransomware victims. In addition to locking their computer systems, the perpetrators notify victims that they have copies of their data and will release sensitive information unless a ransom is paid, extorting them twice. Colonial Pipeline fell victim to the DarkSide ransomware-as-a-service (RaaS) variant. RaaS is a cybercrime model in which one criminal group develops the ransomware and hosts the infrastructure upon which it operates, then leases that capability to another criminal group to conduct an attack.

Pipeline OT operators are exposed to ransomware risks (as are many other industries) to the extent that they have internet-connected IT. In the case of Colonial Pipeline, it was the IT which experienced the ransomware attack. To prevent further potential spread of the attack from the IT systems to their OT systems through some possible (but unknown) pathway, the pipeline operators chose temporarily to disconnect their IT from their OT. Doing so effectively shut down their entire pipeline system.

[6] Tobias Walk, 2012, pp. 7-8.

[7] "The Aurora Project: An Epiphany on Hacking," *SecureTheGrid*, at https://securethegrid.com/destruction-by-cyberattack/.

[8] Jordan Robertson and Michael Riley, "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar," *Bloomberg*, December 10, 2014.

Pipeline Cybersecurity Warnings and Incidents

Federal security officials and industry analysts have long identified pipelines in the United States as potential targets for intentional disruption, although the degree of cyber risk has been steadily growing.[9] For example, a 2011 DHS pipeline threat assessment concluded that "terrorist groups have discussed attacks on unspecified SCADA systems, but it is uncertain whether al-Qa'ida or any other group has the capability to conduct a successful cyberattack on these systems."[10] In 2016, the President of the Association of Oil Pipe Lines testified that cybersecurity threats to pipelines were increasing and that "there is a great concern about … being prepared for cyberattacks."[11] A 2018 Government Accountability Office (GAO) study stated that "new threats to the nation's pipeline systems have evolved to include ... cyberattack or intrusion by nations."[12] In 2019, the President of the Interstate Natural Gas Association of America similarly stated,

> Threats are evolving. Not very long ago, the biggest threats to pipeline operators were the threat of physical damage from a third-party excavator and the threat of financial data compromise from cyber criminals. We now are concerned with the threat from sophisticated, well-resourced nation state actors. These threat actors are motivated and have the technical means to develop zero-day malware that can go undetected in a system for long periods.[13]

Also in 2019, the then-Director of National Intelligence singled out pipelines as critical infrastructure vulnerable to cyberattacks that could cause shutdowns "for days to weeks."[14] On June 6, 2021, the Secretary of Energy stated in an interview, "even as we speak, there are thousands of [cyber]attacks on all aspects of the energy sector."[15]

Growing warnings about pipeline cybersecurity threats have paralleled public reports about significant cyberattacks on U.S. pipelines.

- In March 2012, the Industrial Control Systems Cyber Emergency Response Team within DHS "positively identified" an ongoing series of cyber intrusions among U.S. natural gas pipeline operators dating back to December 2011 as "related to a single campaign."[16] In July 2021, the Cybersecurity and Infrastructure Security Agency and the Federal Bureau of Investigation jointly announced that this

[9] "Already Hard at Work on Security, Pipelines Told of Terrorist Threat," *Inside FERC*, McGraw-Hill Companies, January 3, 2002; Jennifer Alvey, "Cyber Security: A 'Virtual' Reality," *Public Utilities Fortnightly*, September 15, 2003.

[10] Transportation Security Administration, Office of Intelligence, *Pipeline Threat Assessment*, January 18, 2011, p. 3.

[11] Andrew Black, President and CEO, Association of Oil Pipe Lines, testimony before the House Committee on Homeland Security, Transportation and Protective Security Subcommittee hearing on "Pipelines: Securing the Veins of the American Economy," April 19, 2016.

[12] Government Accountability Office (GAO), *Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management*, GAO-19-48, December 2018, p. 1.

[13] Donald Santa, Interstate Natural Gas Association of America, Remarks at the Federal Energy Regulatory Commission Security Investments for Infrastructure Technical Conference, March 28, 2019, https://www.ingaa.org/File.aspx?id=36642&v=62328155. Zero-day malware is malware which is newly discovered or takes advantage of previously unknown vulnerabilities.

[14] Daniel R. Coats, Director of National Intelligence, *Worldwide Threat Assessment of the U.S. Intelligence Community*, January 29, 2019, Statement for the Record before the Senate Select Committee on Intelligence, January 29, 2019, p. 5.

[15] Jennifer Granholm, Secretary of Energy, *Cable News Network (CNN)*, television interview, June 6, 2021.

[16] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), "Gas Pipeline Cyber Intrusion Campaign," *ICS-CERT Monthly Monitor*, April 2012, p. 1.

campaign had targeted 23 pipeline operators. The agencies attributed the attacks to Chinese state-sponsored actors seeking "to help China develop cyberattack capabilities against U.S. pipelines to physically damage pipelines or disrupt pipeline operations."[17]

- In June 2014, a global cybersecurity company reported "an ongoing cyberespionage campaign" by a group known as Dragonfly against "strategically important" U.S. and international targets, primarily in the energy sector, including petroleum pipeline operators.[18]
- In December 2016, the Department of Transportation's (DOT's) Pipeline and Hazardous Materials Safety Administration issued an Advisory Bulletin regarding cybersecurity threats to pipeline SCADA systems, stating that it was "aware of prior intrusion attempts on pipeline infrastructure."[19]
- In March 2018, the DHS Cybersecurity and Infrastructure Security Agency (CISA) issued a cybersecurity alert "on Russian government actions," which included targets in the U.S. energy sector.[20]
- In April 2018, several major U.S. natural gas pipeline companies reported IT cyberattacks on the third-party data interchange systems used to communicate with customers.[21]
- In February 2020, CISA reported "a cyberattack affecting control and communication assets on the operational technology (OT) network of a natural gas compression facility," which led to a two-day pipeline shutdown. According to CISA, "the victim failed to implement robust segmentation between the IT and OT networks, which allowed the adversary to traverse the IT-OT boundary and disable assets on both networks."[22]
- On May 8, 2021, the Colonial Pipeline Company announced that it had halted its pipeline operations due to a ransomware attack, disrupting critical supplies of gasoline and other refined products throughout the East Coast for several days.[23] Although the attack targeted IT systems, the possibility that it could cross over to OT systems led to a precautionary shutdown.

In addition to these incidents, other significant pipeline cyberattacks may have occurred. However, they may not have been reported publicly for reasons including concern about company reputation, data privacy, or system security.

[17] Cybersecurity and Infrastructure Security Agency and Federal Bureau of Investigation, "Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013," Joint Cybersecurity Advisory, Product ID: AA21-201A, July 20, 2021.

[18] A.L. Johnson, "Dragonfly: Western Energy Companies Under Sabotage Threat," Broadcom, cybersecurity blog, June 30, 2014, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks.

[19] PHMSA, "Pipeline Safety: Safeguarding and Securing Pipelines from Unauthorized Access," 81 *Federal Register* 89183, December 9, 2016.

[20] Cybersecurity and Infrastructure Security Agency (CISA), "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," Alert (TA18-074A), March 15, 2018.

[21] R. Collins, N. S. Malik, and M. Vamburkar, "Cyberattack Pings Data Systems of at Least Four Gas Networks," *Bloomberg*, April 4, 2018.

[22] CISA, "Ransomware Impacting Pipeline Operations," Alert (AA20-049A), February 18, 2020.

[23] Colonial Pipeline, "Media Statement Update: Colonial Pipeline System Disruption," May 17, 2021, https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption.

The Federal Role in Pipeline Cybersecurity

There are two federal agencies primarily responsible for pipeline cybersecurity—both part of DHS: the Transportation Security Administration (TSA) and the Cybersecurity and Infrastructure Security Agency (CISA). TSA has broad authorities for pipeline security (physical and cyber) and CISA has broad capabilities for managing cybersecurity risk across a variety of sectors and systems. In addition, other entities, both federal and nongovernmental, have roles in pipeline cybersecurity.

Transportation Security Administration

Federal pipeline security efforts originated in the pipeline safety program. The Natural Gas Pipeline Safety Act of 1968 (P.L. 90-481) and the Hazardous Liquid Pipeline Act of 1979 (P.L. 96-129) are the principal early acts establishing the federal role in pipeline safety. Under both statutes, the Transportation Secretary is given primary authority to regulate key aspects of interstate pipeline safety: design, construction, operation and maintenance, and spill response planning. Presidential Decision Directive 63 (PDD-63), issued by President Bill Clinton in 1998, assigned to DOT the lead responsibility for pipeline security as well as safety.[24] In 2001, President George W. Bush signed the Aviation and Transportation Security Act (P.L. 107-71) establishing the Transportation Security Administration (TSA) within DOT. The act placed the DOT's pipeline security authority (under PDD-63) within TSA. The act specified a range of duties and powers related to general transportation security for TSA, including intelligence management, threat assessment, mitigation, and security measure oversight and enforcement.

In 2002, President George W. Bush signed the Homeland Security Act of 2002 (P.L. 107-296) creating DHS. Among other provisions, the act transferred TSA from DOT to DHS (§403). The Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) directed TSA to promulgate pipeline security regulations and carry out necessary inspection and enforcement if the agency determines that regulations are appropriate (§1557(d)). Thus, TSA has primary responsibility and regulatory authority for the security of natural gas and hazardous liquid (e.g., oil, refined products, and carbon dioxide) pipelines in the United States. In 2018, TSA published its *Cybersecurity Roadmap* to guide the agency's "collective efforts to prioritize cybersecurity measures within TSA."[25] In addition to outlining TSA's own cybersecurity initiatives, the *Roadmap* states that TSA "will work with the Cybersecurity and Infrastructure Security Agency (CISA), with its mission to protect the critical infrastructure of the United States."[26]

Cybersecurity and Infrastructure Security Agency

Congress created CISA in the Cybersecurity and Infrastructure Security Agency Act of 2018 (P.L. 115-278); however, predecessor organizations executed similar authorities and capabilities. Today, CISA's mission is to serve as "the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future."[27] CISA does this for cybersecurity and infrastructure security, and across the two security disciplines. CISA supports pipeline cybersecurity through its Integrated Operations Division and its National Risk Management Center. The Integrated Operations Division contains offices with

[24] Presidential Decision Directive 63, *Protecting the Nation's Critical Infrastructures*, May 22, 1998.

[25] TSA, *Cybersecurity Roadmap 2018*, November 1, 2018.

[26] Ibid., p. 4.

[27] CISA, "About CISA," June 20, 2021, https://www.cisa.gov/about-cisa.

the emergency response capabilities previously held and can conduct vulnerability assessments of ICS at the request of those systems' operators. The National Risk Management Center serves as CISA's planning, analysis, and collaboration center. Among other activities, the center piloted a pipeline cybersecurity initiative to identify and address cybersecurity risks to pipeline systems (discussed further under "TSA Collaboration with CISA").

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

Other Pipeline Cybersecurity Organizations

In addition to TSA and CISA, three other entities play significant roles in pipeline cybersecurity, one federal and two nongovernmental: the Department of Energy's (DOE's) Cybersecurity, Energy Security, and Emergency Response (CESER) office, the Oil and Natural Gas Information Sharing and Analysis Center (ONG-ISAC), and the Downstream Natural Gas Information Sharing and Analysis Center (DNG-ISAC).

The Fixing America's Surface Transportation Act (FAST Act, P.L. 114-94) authorized DOE as the Sector-Specific Agency (i.e., the lead federal agency for security) for the energy sector.[29] The FAST Act also authorized DOE to establish and maintain a capability to manage cybersecurity risks to the energy sector, which DOE executes through CESER. The CESER office funds research and development, deploys monitoring tools to better understand evolving risks, conducts exercises, and coordinates federal responses to energy sector incidents (a role CESER played after the Colonial Pipeline cyberattack).

Pursuant to the Cybersecurity Act of 2015 (P.L. 114-113, Division N), ONG-ISAC and DNG-ISAC are recognized as information sharing and analysis organizations (ISAOs). As such, they can share among their sector membership information on cyber threats and measures to protect against those threats. Additionally, ISAC members can share this information with the government. The ONG-ISAC serves companies in oil and natural gas exploration and production, transportation, refining, and delivery. The DNG-ISAC serves natural gas distribution utilities and pipeline transmission companies. There is some overlap in membership across the two ISACs.

Federal Agency Pipeline Security Activities

TSA and CISA both have active programs in pipeline cybersecurity which encompass a range of related activities. In addition, other federal agencies, including DOT and DOE, support specific aspects of pipeline cybersecurity, either in cooperation with TSA and CISA or independently.

[28] The White House, "Improving Cybersecurity for Critical Infrastructure Control Systems," National Security Memorandum, July 28, 2021, at https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/.

[29] Sector-Specific Agencies for critical infrastructure sectors were designated in Presidential Policy Directive-21, "Critical Infrastructure Security and Resilience," February 12, 2013.

TSA Pipeline Security Program

TSA's pipeline security program currently is administered through the Surface Division in its Office of Security Operations.[30] Although TSA was given regulatory authority for pipeline security under P.L. 107-71 and P.L. 110-53, its activities prior to the Colonial Pipeline cyberattack relied upon voluntary industry compliance with the agency's security guidance and best practice recommendations.[31] In 2003, TSA initiated its ongoing pipeline Corporate Security Review Program, wherein the agency conducts voluntary visits with the largest pipeline and natural gas distribution operators "to assess the current security practices in the pipeline industry, with a focus on the physical and cyber security of pipelines" and the fuels they carry.[32] According to the agency, these reviews typically involve one to three TSA staff meeting with pipeline representatives at the operator's headquarters "to conduct a seven to eight hour interview" to "analyze the owner/operator's security plan and policies and compare their practices with recommendations in TSA's Pipeline Security Guidelines."[33]

P.L. 110-53 also specifically requires TSA to "develop and implement a plan for reviewing the pipeline security plans and an inspection of the critical facilities of the 100 most critical pipeline operators" (§1557(b)). To fulfill this mandate, in 2008 TSA initiated what is now the agency's Critical Facility Security Review Program, under which the agency conducts in-depth physical security reviews of all the critical facilities of the largest pipeline systems in the United States.[34] In this program, pipeline operators identify their own critical facilities based on the TSA Pipeline Security Guidelines. TSA visits these critical facilities and collects site-specific information from operators on facility security policies and procedures, and physical security measures.[35]

Since its formation, TSA has engaged in a number of other pipeline security initiatives, such as developing a statistical tool for risk ranking; publishing a security incident and recovery protocol plan; convening international pipeline security forums; developing pipeline security awareness training materials; convening periodic information-sharing conference calls and classified briefings about pipeline sector threats; and participating in pipeline sector coordinating groups.[36]

Pipeline cybersecurity has long been a distinct focus within TSA's overall pipeline security program. For example, in 2014, TSA was employing the Cybersecurity Assessment and Risk Management Approach in collaborating with stakeholders to identify cyber risks to pipeline industry value chains, critical functions, and supporting cyber infrastructure.[37] TSA's current security guidelines include a dedicated section with cybersecurity provisions.[38] The TSA

[30] TSA, "TSA Organizational Chart," July 21, 2020, https://www.tsa.gov/sites/default/files/tsa_org_chart_matrix.pdf.

[31] Transportation Security Administration (TSA), *Pipeline Security Guidelines*, March 2018 (updated April 2021); and *Pipeline Security Smart Practice Observations*, September 19, 2011.

[32] 84 *Federal Register* 128, July 3, 2019, p. 31896.

[33] Ibid.

[34] The current program originally was established as the Critical Facility Inspection Program. The program was renamed in FY2012 to reflect a change in the program from an inspection to a security review.

[35] 86 *Federal Register* 18291, April 8, 2021, pp. 18291-18292.

[36] Sonya T. Proctor, TSA, testimony before the House Committee on Homeland Security, Subcommittee on Transportation and Maritime Security and Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation, hearing on "Cyber Threats in the Pipeline: Lessons from the Federal Response to the Colonial Pipeline Ransomware Attack," June 15, 2021; Jack Fox, TSA, *Pipeline Security: An Overview of TSA Programs*, slide presentation, May 5, 2014; TSA, *Transportation Systems Sector-Specific Plan*, 2010, p. 326.

[37] Jack Fox, May 5, 2014.

[38] TSA, March 2018, Section 7.

guidelines also state that pipeline operators "should consider the approach outlined" in the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*, other guidance issued by DHS and DOE, and "industry-specific or other established methodologies, standards, and best practices."[39]

TSA Collaboration with CISA

On October 3, 2018, DHS announced the Pipeline Cybersecurity Initiative, which "partners DHS cybersecurity resources, DOE's energy sector expertise, with TSA's regular and ongoing assessments of pipeline security to get a broader understanding of the risks the sector faces."[40] As part of this initiative, TSA began collaborating with CISA's Validated Architecture Design Reviews program in conducting voluntary cybersecurity assessments of pipeline operators. These reviews examine the alignment of pipeline IT or OT infrastructures with federal and industry standards, guidelines, and best practices for cybersecurity through a review of system information provided by pipeline operators and in-person (or virtual) interviews with operator staff.[41] TSA also has cooperated with the Federal Energy Regulatory Commission (FERC), which regulates bulk power system cybersecurity, in conducting voluntary joint Pipeline Cyber Architecture Reviews at select pipeline companies to assess "the pipeline system's cyber security environment of operational and business critical network controls."[42] CISA's Industrial Control Systems Joint Working Group, its National Cybersecurity and Communications Integration Center (NCCIC), and other multi-modal cybersecurity initiatives also involve pipeline operators.[43]

TSA Pipeline Cybersecurity Directives

On May 27, 2021, in response to the Colonial Pipeline cyberattack, TSA issued its first mandatory security requirements in the form of a Security Directive, applicable to owners and operators of critical pipeline facilities (as identified by TSA).[44] The directive requires that these

[39] See National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 16, 2018; and Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, "Cybersecurity Capability Maturity Model (C2M2) Program," https://www.energy.gov/ceser/energy-security/cybersecurity-capability-maturity-model-c2m2-program, accessed June 9, 2021. Relevant industry standards include American Petroleum Institute (API), *Pipeline SCADA Security* (API Standard 1164, currently being updated); and the International Society of Automation and International Electrotechnical Commission (ISA/IEC) 62443 series of standards for industrial automation and control systems, among other standards.

[40] Department of Homeland Security (DHS), "DHS and DOE Meet with Oil and Natural Gas Sector Coordinating Council, Announce Pipeline Cybersecurity Initiative," press release, October 3, 2018.

[41] CISA, "Pipeline Cybersecurity Assessments Update," Oil and Natural Gas Subsector Coordinating Council / Energy Sector Government Coordinating Council Meeting, July 9, 2020, https://www.aga.org/globalassets/virtual-vadr-update-and-vadr_fact-sheet-new-2019.pdf.

[42] David P. Pekoske, TSA Administrator, letter to the Honorable Maria Cantwell, Senate Committee on Commerce, Science, and Transportation, March 21, 2019, https://www.eenews.net/assets/2019/06/27/document_ew_03.pdf; Sonya Proctor, Director, Surface Division, Policy, Plans, and Engagement, TSA, testimony before the House Committee on Homeland Security, Subcommittee on Transportation and Maritime Security, hearing on "Securing U.S. Surface Transportation from Cyber Attacks," February 26, 2019.

[43] CISA, "Industrial Control Systems Joint Working Group (ICSJWG)," https://us-cert.cisa.gov/ics/Industrial-Control-Systems-Joint-Working-Group-ICSJWG; CISA, *Securing Industrial Control Systems: A Unified Initiative*, July 2020, p. 4. The NCCIC incorporates the functions of the former Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

[44] Under 49 U.S.C. §114(l)(2)(A), "if the [TSA] Administrator determines that a regulation or security directive must be issued immediately in order to protect transportation security, the Administrator shall issue the regulation or security directive without providing notice or an opportunity for comment and without prior approval of the Secretary."

companies designate and use a Cybersecurity Coordinator at the corporate level and report any cybersecurity incidents involving their systems to CISA within 12 hours. The directive also required pipeline companies to conduct a cybersecurity vulnerability assessment to determine whether their practices and systems align with TSA's pipeline security guidelines, identify gaps, identify remediation measures that will be taken to fill those gaps, and establish a timeline to implement those measures. Companies were required to report this information to TSA and CISA within 30 days.[45] According to TSA, 100% of companies subject to the directive did so.[46] The directive also states that company information submitted pursuant to the directive will be protected as Sensitive Security Information.[47] The directive is effective for one year but could be extended.[48] TSA's press release announcing the directive further stated that the agency was "also considering follow-on mandatory measures that will further support the pipeline industry in enhancing its cybersecurity."[49]

On June 15, 2021, the TSA Assistant Administrator, Surface Operations, testified that the agency was preparing a second directive with "more specific mitigation measures and ... requirements with regard to assessments," which would be "rather prescriptive in terms of the mitigation measures required." Compliance would be "subject to inspection" by transportation security inspectors who have received training in pipeline operations and cybersecurity from DOT's Pipeline and Hazardous Materials Safety Administration (PHMSA) and Idaho National Laboratory, respectively.[50]

On July 20, 2021, TSA announced its second pipeline cybersecurity directive, requiring critical pipeline owners and operators "to implement specific mitigation measures to protect against ransomware attacks and other known threats to information technology and operational technology systems, develop and implement a cybersecurity contingency and recovery plan, and conduct a cybersecurity architecture design review."[51] TSA's announcement did not provide more specific details because the specific security measures are considered Sensitive Security Information.[52] The TSA Administrator has stated that the NIST Cybersecurity Framework, which is referenced in the second directive, "would give an idea of some of the items that we require," and that the directive also mandates cyber architecture design reviews and contingency planning.[53] The TSA Administrator also has stated that the directive contains provisions whereby operators may seek approval for alternative procedures to any specific measures, providing flexibility for pipeline operators to achieve their intended security outcomes.[54] According to TSA's announcement, CISA advised the agency on pipeline cybersecurity threats and technical

[45] TSA, "Enhancing Pipeline Cybersecurity," Security Directive Pipeline-2021-01, May 27, 2021.

[46] David P. Pekoske, TSA Administrator, testimony before the Senate Committee on Commerce, Science, and Transportation, hearing on "Pipeline Cybersecurity: Protecting Critical Infrastructure," July 27, 2021.

[47] 49 C.F.R. §1520.

[48] Under 49 U.S.C. §114(l)(2)(B), the duration of TSA's security directives may be extended indefinitely if ratified by the Transportation Security Oversight Board.

[49] TSA, "DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators," press release, May 27, 2021.

[50] Sonya T. Proctor, June 15, 2021. Idaho National Laboratory runs the "Critical Infrastructure Protection Training" program. More information available at https://inl.gov/critical-infrastructure-protection-training/.

[51] Department of Homeland Security, "DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators," press release, July 20, 2021.

[52] Sonya T. Proctor, June 15, 2021.

[53] David P. Pekoske, July 27, 2021.

[54] Ibid.

countermeasures during development of the directive. The second directive, like the first, is effective for one year, with the possibility of extension.

DHS and DOT Cooperation

In 2003, President George W. Bush issued Homeland Security Presidential Directive 7 (HSPD-7), clarifying executive agency responsibilities for identifying, prioritizing, and protecting critical infrastructure.[55] HSPD-7 required that DHS and DOT "collaborate in regulating the transportation of hazardous materials by all modes (including pipelines)." Pursuant to this directive, in 2004, the DHS and DOT entered into a memorandum of understanding (MOU) concerning their respective security roles in all modes of transportation. The MOU states that "specific tasks and areas of responsibility that are appropriate for cooperation will be documented in annexes ... individually approved and signed by appropriate representatives of DHS and DOT."[56] In 2006, the agencies signed an annex to the MOU, which was updated in 2020, "to delineate clear lines of authority and responsibility and promote communications, efficiency, and non-duplication of effort ... in the area of transportation security and safety."[57] In March 2010, TSA published a *Pipeline Security and Incident Recovery Protocol Plan* which details the separate and cooperative responsibilities of the two agencies with respect to a pipeline security incident.[58]

DHS and DOT have continued to cooperate on pipeline security in recent years. For example, TSA coordinated with PHMSA and other agencies to address ongoing vandalism and sabotage against critical pipelines by environmental activists in 2016.[59] In April 2016, the Director of TSA's Surface Division testified about the agency's relationship with DOT:

> TSA and DOT co-chair the Pipeline Government Coordinating Council to facilitate information sharing and coordinate on activities including security assessments, training, and exercises. TSA and [PHMSA] work together to integrate pipeline safety and security priorities, as measures installed by pipeline owners and operators often benefit both safety and security.[60]

PHMSA issued a 2016 Advisory Bulletin on SCADA system security "in coordination with" TSA.[61] In July 2017, the two agencies collaborated on a web-based portal to facilitate sharing sensitive but unclassified incident information among federal agencies with pipeline responsibilities.[62] In February 2018, the Director of TSA's Surface Division again testified about

[55] HSPD-7 superseded PDD-63 (par. 37).

[56] Department of Homeland Security (DHS) and Department of Transportation (DOT), *Memorandum of Understanding Between the Department of Homeland Security and the Department of Transportation on Roles and Responsibilities*, September 28, 2004, p. 4.

[57] TSA and PHMSA, "Transportation Security Administration and Pipelines and Hazardous Materials Safety Administration Cooperation on Pipeline Transportation Security and Safety," February 26, 2020. This annex supersedes a prior version of the annex signed in 2006.

[58] TSA, *Pipeline Security and Incident Recovery Protocol Plan*, March 2010, p. 7.

[59] GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management*, GAO-19-48, December 2018, p. 23.

[60] Sonya T. Proctor, Surface Division Director, TSA, testimony before the House Committee on Homeland Security, Subcommittee on Transportation Security hearing on "Pipelines: Securing the Veins of the American Economy," April 19, 2016.

[61] PHMSA, December 9, 2016.

[62] GAO, December 2018, p. 23.

cooperation with PHMSA, stating, "TSA works closely with [PHMSA] for incident response and monitoring of pipeline systems," although she did not provide specific examples.[63]

Following the Colonial Pipeline ransomware attack, PHMSA joined TSA and CISA on a teleconference call with pipeline operators to provide updates on the incident, answer questions, and provide resources to support cybersecurity mitigation efforts.[64] The Deputy Secretary of Transportation subsequently testified that PHMSA intends to "leverage its authorities to inspect and enforce three critical components of pipeline operations" related to cybersecurity: system control room regulations, integrity management plan requirements,[65] and emergency response plan regulations.[66] The Deputy Secretary also stated that DOT's Office of Intelligence, Security, and Emergency Response was collaborating with the National Security Council and interagency partners on a natural gas pipelines Industrial Control Systems Cybersecurity Initiative and that "DOT continues work with [its] sister agencies, especially TSA and CISA, to invest in world class research and pursue initiatives to address cybersecurity threats."[67]

DOE and National Laboratory Activities

DOE administers the Cybersecurity Capability Maturity Model (C2M2) Program, which "enables organizations to voluntarily measure the maturity of their cybersecurity capabilities in a consistent manner."[68] The program has published a sector-specific version of the C2M2 model tailored to the operations of the oil and natural gas industry, including pipelines.[69] DOE also operates the National SCADA Test Bed Program, a partnership with Idaho National Laboratory, Sandia National Laboratories, and other national laboratories to address control system security challenges in the energy sector. Among its key functions, the program performs control system testing, research, and development; control system requirements development; and industry outreach.[70] Sandia Laboratories also has performed authorized defensive cybersecurity assessments examining pipeline systems through its Information Design Assurance Red Team program.[71]

---

[63] Sonya T. Proctor, TSA, testimony before the House Committee on Homeland Security Subcommittee on Transportation and Maritime Security and Subcommittee on Cybersecurity, Infrastructure Protection and Innovation, joint hearing on "Securing U.S. Surface Transportation from Cyber Attacks," February 26, 2019.

[64] TSA, "TSA Response to Congressional Research Service Inquiry on Colonial Pipeline Incident," memorandum, June 29, 2021.

[65] "An integrity management program is a set of safety management, operations, maintenance, evaluation, and assessment processes that are implemented in an integrated and rigorous manner to ensure operators provide enhanced protection for [High-consequence Areas]." See PHMSA, "Overview: Integrity Management," https://primis.phmsa.dot.gov/comm/Im.htm.

[66] Polly Trottenberg, Deputy Secretary of Transportation, written testimony submitted for the Senate Committee on Commerce, Science, and Transportation, hearing on "Pipeline Cybersecurity: Protecting Critical Infrastructure," July 27, 2021, p. 3.

[67] Ibid., pp. 4-5.

[68] DOE, Office of Cybersecurity, Energy Security, and Emergency Response (CESER), "Cybersecurity Capability Maturity Model (C2M2) Program," https://www.energy.gov/ceser/energy-security/cybersecurity-capability-maturity-model-c2m2-program.

[69] DOE, "Cybersecurity Capability Maturity Model, Version 2.0," July 2021.

[70] DOE, Office of Electricity, "National SCADA Test Bed," https://www.energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity/national-scada-test-bed.

[71] See, for example, Sandia National Laboratories, Information Design Assurance Red Team, "Addendum Report: Threat-Based Examination of NAESB Standards and Business Operations," July 15, 2019, https://www.naesb.org/pdf4/bd_cic081419w1.pdf.

GAO Pipeline Security Reports

The TSA Modernization Act, part of the FAA Reauthorization Act of 2018 (P.L. 115-254, Division K, Title I, Subtitle G, §1980) mandated that GAO study the roles and responsibilities of DHS and DOT with respect to pipeline security. The act required examination of "strategic and operational responsibilities for pipeline security" and other specific aspects of TSA's and industry's pipeline security activities (§1980(b)). In response to reporting requirements in the act, GAO published two separate reports, in 2018 and 2019.

GAO's first report, *Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management*, examined TSA's pipeline physical security and cybersecurity program.[72] The report was based upon an analysis of TSA documents, evaluation of TSA's pipeline risk assessments, and interviews with TSA officials, major U.S. pipeline operators, and pipeline industry trade association representatives. Among other findings, GAO's report identified several "weaknesses" in TSA's program management with specific relevance to pipeline cybersecurity.

- Pipeline operators interviewed by GAO reported using a range of guidelines and standards to address physical and cybersecurity risks. All had implemented TSA's voluntary guidelines, although the degree to which they had implemented them was not detailed in the report.
- Although TSA had revised its security guidelines to reflect dynamic threats and incorporate the NIST *Cybersecurity Framework*, the guidelines did not include all of the elements of the framework. TSA also lacked a documented process for regularly reviewing and revising its guidelines, so the agency could not ensure they reflected the latest standards and best practices.
- TSA guidelines lacked clear definitions of what constituted critical facilities, so a number of the largest pipeline system operators "deemed highest risk" had not identified any critical facilities.
- TSA had staffing variations in its pipeline security programs, with the number of full-time equivalent (FTE) employees over a nine-year period ranging between 14 FTEs (FY2012 and FY2013) and 1 FTE (FY2014). There were 6 FTEs in FY2018, the lowest staffing level reported.
- Pipeline operators and industry representatives reported that TSA lacked the expertise required to fully assess cybersecurity in security reviews. TSA did not, at the time, have a strategic workforce plan that identified staffing needs and skill sets such as cybersecurity.
- TSA had not tracked the status of CSR recommendations among pipeline operators for over five years, and related security review data were not sufficiently reliable. Consequently, it was difficult for the agency to evaluate the performance of the pipeline security program.[73]

GAO made 10 recommendations to address the weaknesses it identified in TSA's program. TSA concurred with the recommendations and outlined specific steps it would take to address them. In addition, TSA stated that it would partner with CISA's National Risk Management Center "to

[72] GAO, December 2018.

[73] GAO, December 2018, pp. 28-29, 32, 34, 38-40, 60.

conduct 10 in-depth cybersecurity reviews with pipeline companies during FY2019."[74] As of June 11, 2021, GAO reported that 3 of its 10 recommendations remained outstanding, including its recommendation that TSA "develop a strategic workforce plan ... which could include determining the number of personnel necessary to meet the goals set for its Pipeline Security Branch, as well as the knowledge, skills, and abilities, including cybersecurity."[75] TSA completed the *Final Workforce Assessment Report* in May 2021.[76] The report acknowledged that TSA lacks the qualified personnel with cybersecurity expertise to fully execute TSA's missions.

GAO's second report, *Critical Infrastructure Protection: Key Pipeline Security Documents Need to Reflect Current Operating Environment*, focused on the roles and responsibilities of DHS and DOT in pipeline security.[77] GAO concluded that, while the 2006 TSA-PHMSA MOU Annex delineated the agencies' mutually agreed-upon roles and responsibilities, it had not been reviewed to consider pipeline security developments since its inception. TSA's *Pipeline Security and Incident Recovery Protocol Plan* likewise had not been updated since it was issued in 2010 "to reflect changes in pipeline security threats, technology, federal law and policy, and any other factors."[78] Among other things, GAO recommended that TSA and PHMSA update these documents and put in place formal processes to periodically update them in the future. As noted above, TSA and PHMSA signed an update to the MOU Annex in 2020. In addition, according to GAO, TSA plans to publish an update to its *Pipeline Security and Incident Recovery Protocol Plan* by the end of 2021.[79]

In July 2021, a GAO official testified that TSA had addressed several weaknesses in the management of pipeline security and had fully addressed 12 GAO recommendations identified in the 2018 and 2019 reports. However, according to the testimony, TSA had not fully addressed two cybersecurity-related weaknesses: incomplete information for pipeline risk assessments and aged protocols for responding to pipeline security incidents.[80] With respect to incomplete information, the TSA Administrator subsequently testified that "we oftentimes never have full and complete data, that's very hard to achieve.... [W]e need to move fast ... so we use the best data that we have." However, he agreed with GAO's recommendation and stated that TSA was "working very hard on it."[81]

Issues for Congress

While the federal government has been engaged in various efforts to protect the nation's oil and natural gas pipelines from deliberate cyberattacks since September 11, 2001, questions remain

[74] Ibid., p. 80.

[75] Ibid., p. 62.

[76] U.S. Government Accountability Office, *Critical Infrastructure Protection: TSA is Taking Steps to Address Some Security Program Weaknesses*, GAO-21-105263, July 27, 2021, pp. 12-13, https://www.gao.gov/assets/gao-21-105263.pdf.

[77] GAO, *Critical Infrastructure Protection: Key Pipeline Security Documents Need to Reflect Current Operating Environment*, GAO-19-426, June 2019.

[78] Ibid., pp. 29-30.

[79] Leslie V. Gordon, June 11, 2021.

[80] Leslie V. Gordon, "Critical Infrastructure Protection: TSA Is Taking Steps to Address Some Pipeline Security Program Weaknesses," written testimony submitted for the Senate Committee on Commerce, Science, and Transportation hearing on "Pipeline Cybersecurity: Protecting Critical Infrastructure," GAO-21-105263, July 27, 2021, pp. 11, 14.

[81] David P. Pekoske, July 27, 2021.

regarding the structure and effectiveness of these efforts. Five specific issues, in particular, have raised concern and may warrant further congressional consideration: (1) TSA's pipeline cybersecurity resources, (2) the nature of federal cybersecurity standards, (3) roles and coordination among federal entities involved in pipeline cybersecurity, (4) uncertainty about cybersecurity threats to the nation's pipeline network, and (5) coordinating a national pipeline strategy.

TSA Pipeline Cybersecurity Staffing Resources

The sufficiency of staff funding and resources to implement the nation's pipeline security program has been a concern of Congress almost since DHS was established. For example, one Senator remarked in 2005 that "aviation security has received 90% of TSA's funds and virtually all of its attention. There is simply not enough being done to address ... pipeline security."[82] At a hearing in April 2010, a Member likewise expressed concern that TSA's pipeline division did not have sufficient staff to carry out a federal pipeline security program on a national scale.[83] According to GAO's 2019 report, TSA itself acknowledged that staffing limitations had prevented the agency from conducting more pipeline security reviews.[84] In February 2019, TSA had five FTE staff in pipeline security, none with "specific cybersecurity expertise," according to the agency.[85]

On June 15, 2021, the TSA Assistant Administrator testified that TSA's pipeline security staffing would increase in FY2021 "to 34 positions working in field operations, headquarters operations, and policy development," although some of these positions had yet to be filled. Of these 34 positions, 6 would be for "specialized cybersecurity personnel," in a new Cybersecurity Operations Support Branch, with another 5 cybersecurity specialists to be hired into the branch in FY2022. TSA's Surface Policy Division also plans to have 9 FTEs in the Cybersecurity Section of its Office of Policy, Plans, and Engagement by the end of FY2021 to "focus on the development of cybersecurity-related policy and guidance for surface transportation security."[86]

The TSA Assistant Administrator also testified that the agency currently has the funding and personnel needed to ensure accountability for pipeline operator cybersecurity.[87] Nonetheless, it is uncertain whether the agency, as currently staffed and structured, could develop and implement new security regulations (if needed), conduct rigorous security plan verification, follow up with effective enforcement, and maintain currency regarding the cybersecurity threat environment. Developing and implementing more prescriptive cybersecurity regulations could pose a particular challenge to agency resources, depending upon the process (e.g., directives, rulemaking), nature, and extent of such regulations.

[82] Sen. Daniel K. Inouye, opening statement before the Senate Committee on Commerce, Science, and Transportation hearing on the President's FY2006 Budget Request for the Transportation Security Administration, February 15, 2005.

[83] Rep. Gus M. Bilirakis, Remarks Before the House Committee on Homeland Security, Subcommittee on Management, Investigations, and Oversight hearing on "Unclogging Pipeline Security: Are the Lines of Responsibility Clear?," Plant City, FL, April 19, 2010.

[84] GAO, December 2018, p. 38.

[85] Sonya T. Proctor, February 26, 2019.

[86] Sonya T. Proctor, June 15, 2021.

[87] Ibid.

Cybersecurity Standards

There continues to be debate in Congress about the adequacy of a voluntary standards approach to cybersecurity within the pipeline sector (as well as other critical infrastructure sectors). Prior to the May 2021 Colonial Pipeline cyberattack, TSA used a voluntary approach to pipeline security generally, and to cybersecurity specifically, as discussed above. This approach was controversial. For example, as early as 2008, a DOT Inspector General report stated that "TSA's current security guidance is not mandatory and remains unenforceable unless a regulation is issued to require industry compliance."[88] The issue of whether to have voluntary or mandatory standards has arisen often over the last decade. Some stakeholders have advocated for mandatory standards to ensure compliance and others, notably the pipeline industry and TSA, have asserted that the voluntary standards approach has been effective.[89]

TSA has started to move past voluntary compliance. Following the Colonial Pipeline attack, the agency issued its two security directives requiring critical operators to have a cybersecurity coordinator, report incidents, assess cyber vulnerability, and implement prescriptive measures and practices to defend against cyber threats. However, under the TSA's directives, questions may arise about how pipeline operators fulfill their cybersecurity requirements. In particular, there is debate about the relative suitability and efficacy of prescriptive standards versus performance standards in the pipeline sector. Prescriptive standards mandate particular means (e.g., specific types of hardware or software). Performance standards establish goals that entities must achieve (e.g., continuous monitoring) but allow entities to individually decide how to achieve those goals. A voluntary or mandatory standard can be either prescriptive or performance-based.

According to TSA officials, the agency's second directive imposes more prescriptive cybersecurity mitigation requirements on operators. TSA's announcement of the directive stated that it was mandating "urgently needed protections" to "better ensure the pipeline sector takes the steps necessary to safeguard their operations from rising cyber threats."[90] However, some in the pipeline sector have criticized the second directive as overly prescriptive and as having been promulgated under emergency authority without a traditional rulemaking process with more industry input.[91] As TSA evaluates its current security directives for pipelines and considers additional directives or rules, the balance of voluntary vs. mandatory and prescriptive vs. performance standards may continue to be an issue for Congress.

Roles of Federal Entities and Agency Coordination

Some Members of Congress and other stakeholders have questioned whether aspects of the federal program for pipeline security, especially cybersecurity, should be administered by an agency other than TSA. Concerns with TSA have centered on the adequacy of personnel and expertise, industry relationships, and experience with regulatory programs. For example, in 2018, two FERC commissioners asserted that the program should be moved to an agency that "fully

[88] U.S. Dept. of Transportation, Office of Inspector General, May 21, 2008, p. 6. Provisions in the Pipeline Inspection, Protection, Enforcement, and Safety Act of 2006 (P.L. 109-468) required the Inspector General to "address the adequacy of security standards for gas and oil pipelines" (§23(b)(4)).

[89] See, for example, testimony before the Senate Committee on Commerce, Science, and Transportation hearing on "Transportation Security Administration Oversight: Confronting America's Transportation Security Challenges," April 30, 2014.

[90] Department of Homeland Security, July 20, 2021.

[91] Leticia Gonzales, "TSA Adds More Stringent Cybersecurity Requirements for U.S. Natural Gas, Oil Pipelines," *Natural Gas Intelligence*, July 23, 2021.

comprehends the energy sector and has sufficient resources to address this growing threat." The commissioners specifically proposed DOE as a more "appropriate" place for the program because DOE is the Sector-Specific Agency for energy security and also administers CESER.[92] Other stakeholders have suggested that PHMSA might be a more suitable agency to administer the pipeline security program due to its greater resources, pipeline expertise, long-standing relationships with operators, and existing pipeline safety regulatory program.[93] Still others have expressed support for TSA's continued oversight of pipeline cybersecurity. Among other reasons, they cite the agency's recent expansion of staffing dedicated to pipeline cybersecurity, its collaboration with CISA, and other organizational changes.

Pending legislative proposals pertain to the role of TSA and other federal agencies in pipeline cybersecurity. They seek to recodify TSA's cybersecurity role (e.g., Pipeline Security Act, H.R. 3243) and to require the Secretary of Energy to carry out certain responsibilities for pipeline cybersecurity (e.g., Pipeline and LNG Facility Cybersecurity Preparedness Act, H.R. 3078). Another bill, the Promoting Interagency Coordination for Review of Natural Gas Pipelines Act (H.R. 1616), would require FERC to consult with TSA in reviewing interstate natural gas pipeline permit applications regarding an applicant's compliance with TSA's pipeline cybersecurity standards and recommendations. Recently enacted measures and actions include passage of the PIPEs Act of 2020 (P.L. 116-260, Division R) reauthorizing PHMSA's pipeline safety program, the FAST Act (P.L. 114-94) authorizing DOE's responsibility for energy delivery cybersecurity, and the 2016 U.S. Coast Guard/NIST partnership on cyber risk management for the transfer of hazardous liquids from marine vessels to onshore pipelines.[94]

During a 2021 budget hearing of the Senate Committee on Energy and Natural Resources with the Secretary of Energy, Senators raised concerns about the multiagency oversight of pipeline cybersecurity.[95] Concerns include the opportunities for gaps and oversight without a single agency in charge. Conversely, other Members have suggested keeping the current multiagency approach since it encourages agencies to focus capabilities on areas where they have the greatest expertise.[96] As Congress further examines federal roles for pipeline cybersecurity, it may evaluate the breadth of agencies' pipeline authorities (e.g., security as a whole, or exclusively cybersecurity), the location in the federal government of cyber-specific capabilities, the capacity of those capabilities, and the mechanisms agencies employ to coordinate capabilities.

Pipeline Cybersecurity Threat Information

Concerns about the quality and specificity of federal threat information have long been an issue across critical infrastructure sectors.[97] Threat information continues to be a key concern in the

[92] Neil Chatterjee and Richard Glick, "Cybersecurity Threats to U.S. Gas Pipelines Call for Stricter Oversight," *Axios*, June 11, 2018.

[93] See, for example, Blake Sobczak, "Battle Lines Form over Pipeline Cyberthreat," *E&E News*, July 25, 2019.

[94] U.S. Coast Guard, "Maritime Bulk Liquid Transfer Cybersecurity Framework Profile," 2016, at https://www.dco.uscg.mil/Portals/9/CG-FAC/Documents/Maritime_BLT_CSF.pdf?ver=2017-07-19-070544-223.

[95] U.S. Congress, Senate Committee on Energy and Natural Resources, *The President's Budget Request for the Department of Energy for Fiscal Year 2022*, 117th Cong., 1st sess., June 15, 2021.

[96] U.S. Congress, House Committee on Homeland Security, Subcommittees on Transportation and Maritime Security, and Cybersecurity, Infrastructure Protection, and Innovation, *Cyber Threats in the Pipeline: Lessons from the Federal Response to the Colonial Pipeline Ransomware Attack*, 117th Cong., 1st sess., June 15, 2021.

[97] See, for example, Philip Shenon, "Threats and Responses: Domestic Security," *New York Times*, June 5, 2003, p. A15.

case of pipeline cybersecurity.[98] The pipeline industry's cybersecurity assessments rely upon information about cybersecurity threats provided by the federal government and by pipeline operators themselves. The quantity, quality, and timeliness of this threat information are key determinants of which threats pipeline companies protect against, and which security measures are taken. Incomplete or ambiguous threat information—especially from the federal government—may lead to inconsistency in cybersecurity mitigation among pipeline owners, inefficient spending of security resources at facilities, or deployment of security measures against the wrong threat.

Questions for Congress related to pipeline cybersecurity threat information include the following:

- Which agency (or agencies) should be responsible for collecting, analyzing, and/or disseminating threat information?
- Which agency (or agencies) should be responsible for developing mitigating strategies to cybersecurity threats?
- Does the intelligence community need to improve collection about adversary targeting of critical infrastructure?
- How will the government track the disposition of information shared and assess the efficacy of information-sharing programs?
- Is classified information a barrier to information sharing, or is pertinent information able to be disseminated in an unclassified manner?
- Has the cyber risk information-sharing model authorized in the Cybersecurity Act of 2015 (P.L. 114-113, Division N) been successful, or do barriers exist to effective information sharing among sector partners? The model in the act involves sector-wide information sharing through information sharing and analysis organizations.

Congress examined aspects of these issues during the first session of the 117th Congress. For example, during a hearing of the Senate Committee on Commerce, Science, and Transportation on pipeline cybersecurity, federal officials asserted a need for "trusted and timely" information sharing among both public- and private-sector partners.[99] Also, a hearing by the House Committee on Energy and Commerce highlighted an example of challenges to information sharing: the government may share classified information with a company's executive, but that executive may lack cleared personnel in the company who can then take action on the information because of its classification.[100]

Coordinating a National Pipeline Cybersecurity Strategy

In addition to the specific issues highlighted above, Congress may assess how the various elements of U.S. pipeline cybersecurity and critical infrastructure security will fit together most effectively in the nation's overall strategy to protect critical pipelines. Pipeline security necessarily involves various groups: federal agencies, pipeline associations, large and small

[98] U.S. Congress, House Committee on Homeland Security, *Cyber Threats in the Pipeline: Using Lessons from the Colonial Pipeline Ransomware Attack to Defend Critical Infrastructure*, 117th Cong., 1st sess., June 9, 2021.

[99] U.S. Congress, Senate Committee on Commerce, Science, and Transportation, *Pipeline Cybersecurity: Protecting Critical Infrastructure*, 117th Cong., 1st sess., July 21, 2021.

[100] U.S. Congress, House Committee on Energy and Commerce, Subcommittee on Energy, *FERC Oversight*, 117th Cong., 1st sess., July 27, 2021.

pipeline operators, and the broader industrial cybersecurity community. Reviewing how these groups work together to achieve common goals could be an overarching challenge for Congress.

Author Information

Paul W. Parfomak
Specialist in Energy Policy

Chris Jaikaran
Analyst in Cybersecurity Policy

Disclaimer