

PIPELINE CYBERSECURITY: PROTECTING CRITICAL INFRASTRUCTURE

HEARING

BEFORE THE

COMMITTEE ON COMMERCE,
SCIENCE, AND TRANSPORTATION
UNITED STATES SENATE

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

JULY 27, 2021

Printed for the use of the Committee on Commerce, Science, and Transportation



Available online: <http://www.govinfo.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

WASHINGTON : 2023

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

MARIA CANTWELL, Washington, *Chair*

AMY KLOBUCHAR, Minnesota	ROGER WICKER, Mississippi, <i>Ranking</i>
RICHARD BLUMENTHAL, Connecticut	JOHN THUNE, South Dakota
BRIAN SCHATZ, Hawaii	ROY BLUNT, Missouri
EDWARD MARKEY, Massachusetts	TED CRUZ, Texas
GARY PETERS, Michigan	DEB FISCHER, Nebraska
TAMMY BALDWIN, Wisconsin	JERRY MORAN, Kansas
TAMMY DUCKWORTH, Illinois	DAN SULLIVAN, Alaska
JON TESTER, Montana	MARSHA BLACKBURN, Tennessee
KYRSTEN SINEMA, Arizona	TODD YOUNG, Indiana
JACKY ROSEN, Nevada	MIKE LEE, Utah
BEN RAY LUJAN, New Mexico	RON JOHNSON, Wisconsin
JOHN HICKENLOOPER, Colorado	SHELLEY MOORE CAPITO, West Virginia
RAPHAEL WARNOCK, Georgia	RICK SCOTT, Florida
	CYNTHIA LUMMIS, Wyoming

DAVID STRICKLAND, *Staff Director*

MELISSA PORTER, *Deputy Staff Director*

GEORGE GREENWELL, *Policy Coordinator and Security Manager*

JOHN KEAST, *Republican Staff Director*

CRYSTAL TULLY, *Republican Deputy Staff Director*

STEVEN WALL, *General Counsel*

CONTENTS

Hearing held on July 27, 2021	Page 1
Statement of Senator Cantwell	1
GAO report dated December 18, 2018, entitled, “Critical Infrastructure Protection Actions Needed”	2
<i>New York Times</i> article dated May 14, 2021 entitled, “Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity” by David E. Sanger and Nicole Perlroth	57
Article dated May 11, 2021, entitled, “Colonial Pipeline hack highlights grid disruption risks even with IT-focused cyberattack, analysts say” by Robert Walton, Reporter, Utility Dive	60
Article dated May 13, 2021, entitled, “Colonial Pipeline Cyber Attack Highlights Need For More Seriousness In Energy Policy” by David Blackmon, Senior Editor, Shale Magazine	86
Article dated June 18, 2018, entitled, “Cyber security rules needed for pipelines: FERC commissioners” by Neil Chatterjee, Richard Glick, Federal Energy Regulatory Commission	89
Statement of Senator Wicker	55
Statement of Senator Klobuchar	94
Statement of Senator Thune	96
Statement of Senator Fischer	98
Statement of Senator Markey	99
Statement of Senator Blumenthal	101
Statement of Senator Blackburn	103
Statement of Senator Capito	105
Statement of Senator Rosen	107
Statement of Senator Tester	109
Statement of Senator Hickenlooper	110
Statement of Senator Scott	112
Statement of Senator Warnock	114

WITNESSES

Hon. David P. Pekoske, Administrator, Transportation Security Administra- tion	65
Prepared statement	67
Hon. Polly Trottenberg, Deputy Secretary, Department of Transportation	70
Prepared statement	72
Leslie V. Gordon, Acting Director, Homeland Security and Justice, Govern- ment Accountability Office	74
Prepared statement	75

APPENDIX

Response to written questions submitted to Hon. David P. Pekoske by:	
Hon. Maria Cantwell	119
Hon. Kyrsten Sinema	120
Hon. Ben Ray Luján	122
Hon. Marsha Blackburn	123
Response to written questions submitted to Hon. Polly Trottenberg by:	
Hon. Maria Cantwell	123
Hon. Tammy Duckworth	125
Hon. Kyrsten Sinema	126
Hon. Ron Johnson	129
Response to written questions submitted to Leslie V. Gordon by:	
Hon. Marsha Blackburn	130

PIPELINE CYBERSECURITY: PROTECTING CRITICAL INFRASTRUCTURE

TUESDAY, JULY 27, 2021

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 10 a.m. in room SR-253, Russell Senate Office Building, Hon. Maria Cantwell, Chairwoman of the Committee, presiding.

Present: Senators Cantwell [presiding], Klobuchar, Blumenthal, Markey, Tester, Rosen, Hickenlooper, Warnock, Wicker, Thune, Fischer, Blackburn, Capito, and Scott.

OPENING STATEMENT OF HON. MARIA CANTWELL, U.S. SENATOR FROM WASHINGTON

The CHAIRMAN. Good morning. The Senate Committee on Commerce, Science, and Transportation will come to order. We very much appreciate the witnesses being here.

Earlier this year the ransomware attack on Colonial Pipeline caused the company to shut down its pipeline system that supplies nearly 50 percent of fuel to the East Coast. This resulted in gas shortages causing spikes, causing prices to spike and panic buying from Georgia to New York.

Although service was restored within a week, the incident underscores the potential consequence of any single cyber attack can have on our daily lives and the need to better manage and bolster our cybersecurity for our critical infrastructure.

Our nation relies on more than 2.8 million miles of pipeline, 140,000 miles of railroad track, four million miles of roads, 11 million trucks, airport supports, and the infrastructure increasingly depends on information technology systems, electronic data that is very susceptible to cyber threats.

The Colonial Pipeline attack is, frankly, the tip of the iceberg. Our country is seeing 4,000 ransomware attacks every single day and since the start of the coronavirus pandemic, the FBI reported that cyber attacks have increased over 300 percent.

The rapid growth in the number of sophisticated cyber attacks is an alarm bell ringing about the need to immediately bolster cybersecurity of our critical infrastructure.

If we don't, it will only be a matter of time before we see another crippling cyber incident that will have an even more catastrophic impact on what we saw with Colonial Pipeline and the pipelines are not the only vulnerable infrastructure in this country that is vulnerable to this level of serious disruption.

For years experts have been worried about the vulnerability of our Nation's grid to the disruptions from nefarious actors, including from cyber attacks.

I want to enter into the record "Critical Infrastructure Protection Actions Needed" that was a GAO report that was done in December 2018.

[The information referred to follows]



United States Government Accountability Office

Report to Congressional Requesters

December 2018

CRITICAL INFRASTRUCTURE PROTECTION

Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management

GAO Highlights

Highlights of GAO-19-48, a report to congressional requesters

Why GAO Did This Study

More than 2.7 million miles of pipeline transport and distribute oil, natural gas, and other hazardous products throughout the United States. Interstate pipelines run through remote areas and highly populated urban areas, and are vulnerable to accidents, operating errors, and malicious physical and cyber-based attack or intrusion. The energy sector accounted for 35 percent of the 796 critical infrastructure cyber incidents reported to DHS from 2013 to 2016. Several federal and private entities have roles in pipeline security. TSA is primarily responsible for the oversight of pipeline physical security and cybersecurity.

GAO was asked to review TSA's efforts to assess and enhance pipeline security and cybersecurity. This report examines, among other objectives: (1) the guidance pipeline operators reported using to address security risks and the extent that TSA ensures its guidelines reflect the current threat environment; (2) the extent that TSA has assessed pipeline systems' security risks; and (3) the extent TSA has assessed its effectiveness in reducing pipeline security risks.

GAO analyzed TSA documents, such as its *Pipeline Security Guidelines*; evaluated TSA pipeline risk assessment efforts; and interviewed TSA officials, 10 U.S. pipeline operators—selected based on volume, geography, and material transported—and representatives from five industry associations.

What GAO Recommends

GAO makes 10 recommendations to TSA to improve its pipeline security program management (many are listed on the next page), and DHS concurred.

View GAO-19-48. For more information, contact Chris Currie at (404) 679-1875 or currie@gao.gov and Nick Marinov at (202) 512-9342 or marinov@gao.gov.

December 2018

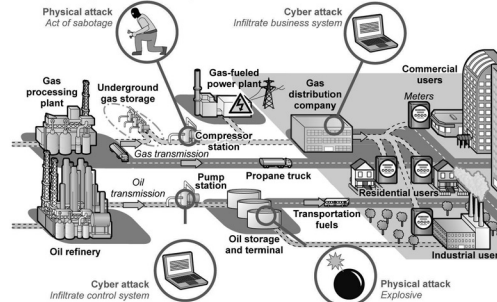
CRITICAL INFRASTRUCTURE PROTECTION

Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management

What GAO Found

Pipeline operators reported using a range of guidelines and standards to address physical and cybersecurity risks, including the Department of Homeland Security's (DHS) Transportation Security Administration's (TSA) *Pipeline Security Guidelines*, initially issued in 2011. TSA issued revised guidelines in March 2018 to reflect changes in the threat environment and incorporate most of the principles and practices from the National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity*. However, TSA's revisions do not include all elements of the current framework and TSA does not have a documented process for reviewing and revising its guidelines on a regular basis. Without such a documented process, TSA cannot ensure that its guidelines reflect the latest known standards and best practices for physical security and cybersecurity, or address the dynamic security threat environment that pipelines face. Further, GAO found that the guidelines lack clear definitions to ensure that pipeline operators identify their critical facilities. GAO's analysis showed that operators of at least 34 of the nation's top 100 critical pipeline systems (determined by volume of product transported) deemed highest risk had identified no critical facilities. This may be due, in part, to the guidelines not clearly defining the criteria to determine facilities' criticality.

U.S. Pipeline Systems' Basic Components and Vulnerabilities



Source: GAO analysis of Transportation Security Administration information. | GAO-19-48

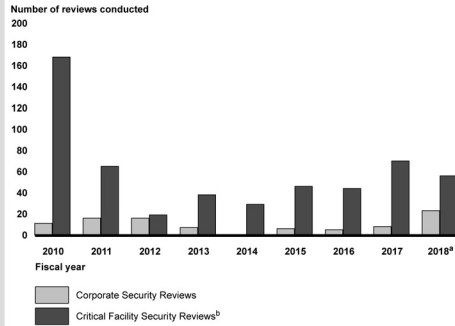
To assess pipeline security risks, TSA conducts pipeline security reviews—Corporate Security Reviews and Critical Facility Security Reviews—to assess pipeline systems' vulnerabilities. However, GAO found that the number of TSA security reviews has varied considerably over the last several years, as shown in the table on the following page.

What GAO Recommends

GAO recommends, among other things, that the TSA Administrator take the following actions:

- implement a documented process for reviewing, and if deemed necessary, for revising TSA's *Pipeline Security Guidelines* at defined intervals;
- clarify TSA's *Pipeline Security Guidelines* by defining key terms within its criteria for determining critical facilities;
- develop a strategic workforce plan for TSA's Security Policy and Industry Engagement's Surface Division;
- update TSA's pipeline risk assessment methodology to include current data to ensure it reflects industry conditions and threats;
- fully document the data sources, underlying assumptions and judgments that form the basis of TSA's pipeline risk assessment methodology;
- take steps to coordinate an independent, external peer review of TSA's pipeline risk assessment methodology;
- ensure the Security Policy and Industry Engagement's Surface Division has a suite of performance measures which exhibit key attributes of successful performance measures; and
- enter information on Corporate Security Review recommendations and monitor and record their status.

Pipeline Security Reviews Conducted, Fiscal Year 2010 through July 2018



Source: GAO analysis of Transportation Security Administration-reported figures. | GAO-19-48

^aFiscal year 2018 data are through July 31, 2018.

^bFiscal years 2010 and 2011 represent Critical Facility Inspections—the predecessor of the Critical Facility Security Review.

TSA officials stated that staffing limitations have prevented TSA from conducting more reviews. Staffing levels for TSA's Pipeline Security Branch have varied significantly since fiscal year 2010 with the number of staff ranging from 14 full-time equivalents in fiscal years 2012 and 2013 to 1 in 2014. Further, TSA does not have a strategic workforce plan to help ensure it identifies the skills and competencies—such as the required level of cybersecurity expertise—necessary to carry out its pipeline security responsibilities. By establishing a strategic workforce plan, TSA can help ensure that it has identified the necessary skills, competencies, and staffing.

GAO also identified factors that likely limit the usefulness of TSA's risk assessment methodology for prioritizing pipeline system reviews. Specifically, TSA has not updated its risk assessment methodology since 2014 to reflect current threats to the pipeline industry. Further, its sources of data and underlying assumptions and judgments regarding certain threat and vulnerability inputs are not fully documented. In addition, the risk assessment has not been peer reviewed since its inception in 2007. Taking steps to strengthen its risk assessment, and initiating an independent, external peer review would provide greater assurance that TSA ranks relative risk among pipeline systems using comprehensive and accurate data and methods.

TSA has established performance measures to monitor pipeline security review recommendations, analyze their results, and assess effectiveness in reducing risks. However, these measures do not possess key attributes—such as clarity, and having measurable targets—that GAO has found are key to successful performance measures. By taking steps to ensure that its pipeline security program performance measures exhibit these key attributes, TSA could better assess its effectiveness at reducing pipeline systems' security risks. Pipeline Security Branch officials also reported conducting security reviews as the primary means for assessing the effectiveness of TSA's efforts to reduce pipeline security risks. However, TSA has not tracked the status of Corporate Security Review recommendations for the past 5 years. Until TSA monitors and records the status of these reviews' recommendations, it will be hindered in its efforts to determine whether its recommendations are leading to significant reduction in risk.

December 18, 2018

Congressional Requesters

The security of the Nation's pipeline systems is vital to public confidence and the Nation's safety, prosperity, and well-being. More than 2.7 million miles of pipeline transport and distribute the oil, natural gas, and other hazardous liquids that U.S. citizens and businesses depend on to operate vehicles and machinery, heat homes, generate electricity, and manufacture products. The interstate pipeline system runs through remote, as well as highly populated urban areas, and is vulnerable to accidents, operating errors, and malicious attacks. In addition, pipelines increasingly rely on sophisticated networked computerized systems and electronic data, which are vulnerable to cyber attack or intrusion.

Given that many pipelines transport volatile, flammable, or toxic oil and liquids, and given the potential consequences of a successful physical or cyber attack on life, property, the economy, and the environment, pipeline systems are attractive targets for terrorists, hackers, foreign nations, criminal groups, and others with malicious intent. For example, according to the Transportation Security Administration (TSA)—the Federal agency with responsibility for security in all modes of transportation, which includes the oversight of pipeline physical security and cybersecurity—a minor pipeline system disruption could result in commodity price increases while prolonged pipeline disruptions could lead to widespread energy shortages.¹ Further, disruption of any magnitude may affect other domestic critical infrastructure and industries that are dependent on pipeline system commodities.

Since the September 11, 2001, terrorist attacks, new threats to the Nation's pipeline systems have evolved to include sabotage by environmental activists and cyber attack or intrusion by nations.² In October 2016, environmental activists forced the shutdown of five crude oil pipelines in four states.³ In addition, the U.S. energy sector has experienced cyber intrusions by nation-state actors into their networks. For example, in March 2018, the Federal Bureau of Investigation and the National Cybersecurity and Communications Integration Center (NCCIC) reported that a nation-state had targeted organizations within multiple U.S. critical infrastructure sectors, including the energy sector, and collected information pertaining to Industrial Control Systems (ICS).⁴ Also, in April 2012, the Industrial Control Systems Cyber Emergency Response Team reported that an unidentified cyber attacker had conducted a series of cyber intrusions into U.S. natural gas pipeline systems beginning in December 2011.⁵

The security of Federal cyber assets has been on our High Risk list since 1997 and was expanded to include the protection of critical cyber infrastructure in 2003.⁶ In September 2018, we issued an update to the information security high-risk area that identified actions needed to address cybersecurity challenges facing the Nation.⁷ We last reported on pipeline security in 2010 and made eight recommendations to TSA to develop outcome-based performance measures for assessing TSA's pipeline security efforts, and to track its corporate security reviews and critical facil-

¹Transportation Security Administration, *Biennial National Strategy for Transportation Security: Report to Congress* (Washington, D.C.: Apr. 4, 2018).

²Nations, including nation-state, state-sponsored, and state-sanctioned programs, use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities.

³Congressional Research Service, *Pipeline Security: Recent Attacks*, IN106103 (Washington, D.C.: Apr. 11, 2017).

⁴Federal Bureau of Investigation and National Cybersecurity and Communications Integration Center, *Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors*, TA18-074A (Washington, D.C.: Mar., 16, 2018 (revised)). Industrial control systems include software-based systems used to monitor and control many aspects of network operation for pipeline networks.

⁵Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), *ICS-CERT Monthly Monitor* (Washington, D.C.: Apr. 2012).

⁶Our biennial High Risk List identifies government programs that have greater vulnerability to fraud, waste, abuse, and mismanagement or need to address challenges to economy, efficiency, or effectiveness. We have designated Federal information security as a High Risk area since 1997; in 2003, we expanded this high risk area to include protecting systems supporting our Nation's critical infrastructure; and, in 2015, we further expanded this area to include protecting the privacy of personally identifiable information that is collected, maintained, and shared by both Federal and nonfederal entities. See GAO, *High Risk Series: Progress on Many High Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317 (Washington, D.C.: Feb. 15, 2017).

⁷GAO, *High Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Washington, D.C.: Sept. 6, 2018).

ity inspections' recommendations,⁸ among others.⁹ We discuss some of these recommendations in more detail later in this report. In 2012, we reviewed information provided by TSA and closed the recommendations as implemented.

You requested that we review TSA's efforts to enhance pipeline physical security and cybersecurity. This report examines the following objectives:

1. how do pipeline sector stakeholders share security-related information;
2. what guidance do pipeline operators report using to address security risks and to what extent does TSA ensure its guidelines reflect the current threat environment;
3. to what extent has TSA assessed security risks to pipeline systems; and
4. to what extent has TSA assessed its effectiveness in reducing pipeline security risks.

For each objective, we interviewed representatives of the five major associations with ties to the pipeline industry: the American Petroleum Institute (API), the Association of Oil Pipe Lines, the American Gas Association (AGA), the Interstate Natural Gas Association of America (INGAA), and the American Public Gas Association. We also interviewed a nonprobability sample of security personnel from 10 pipeline operators. We selected the 10 pipeline operators from TSA's list of the top 100 critical pipeline systems.¹⁰ We chose operators to ensure a mixture of the following characteristics: (a) type of pipeline commodity transported (*i.e.*, natural gas or hazardous oil and liquids); (b) volume of product transported; and (c) whether or not the pipeline operators' critical facilities had been the subject of a TSA security review. We also considered the location of selected operators' pipeline systems to ensure that a single state or region was not overrepresented in our sample. We then conducted semistructured interviews to obtain operators' perspectives on pipeline security and the role of Federal agencies in assisting operators with security activities. While the information gathered during operator interviews cannot be generalized to all pipeline operators, it provides a range of perspectives on a variety of topics relevant to pipeline security.

To identify how pipeline sector stakeholders share security-related information, we reviewed documents describing Federal agencies' processes for sharing security-related information with Federal partners and private industry. In addition, we reviewed relevant documents from TSA and other Federal entities, including the Department of Transportation (DOT), DOT's Pipeline and Hazardous Materials Safety Administration (PHMSA), the Department of Energy (DOE), and the Federal Energy Regulatory Commission (FERC). We also interviewed agency and industry officials to gather their perspectives on how security information is shared among pipeline sector stakeholders.

To identify the guidance pipeline operators report using to address security risks and the extent to which TSA ensures its guidelines reflect the current threat environment, we reviewed TSA's 2018 *Pipeline Security Guidelines*¹¹ and compared the cybersecurity-related sections to applicable standards of the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*.¹² We also interviewed Federal officials to identify security-related standards and guidance issued. In addition, we obtained from industry officials the

⁸TSA conducts two types of pipeline security reviews: Corporate Security Reviews and Critical Facility Security Reviews. Corporate Security Reviews are voluntary on-site reviews of a pipeline owner's corporate policies and procedures. Critical Facility Security Reviews are voluntary on-site inspections of critical pipeline facilities, as well as other select pipeline facilities, throughout the Nation. Critical Facility Inspections were the predecessor to Critical Facility Security Reviews.

⁹GAO, *Pipeline Security: TSA Has Taken Actions to Help Strengthen Security, but Could Improve Priority-Setting and Assessment Processes*, GAO-10-867 (Washington, D.C.: Aug. 2010).

¹⁰According to TSA, a system is considered critical if it is so vital to the United States that its incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof. TSA determines the top 100 most critical pipeline systems based on the amount of hazardous liquid or natural gas product transported through a pipeline in 1 year.

¹¹Transportation Security Administration, *Pipeline Security Guidelines* (March 2018).

¹²National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0* (Gaithersburg, Md.: Feb. 12, 2014). In response to Executive Order 13636, NIST issued the *Framework for Critical Infrastructure Cybersecurity*, which is intended to help organizations apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. The framework consists of five concurrent and continuous functions: identify, protect, detect, respond, and recover. When considered together, these functions provide a high-level, strategic view of the life cycle of an organization's management of cybersecurity risk.

security-related standards and guidance they use and asked them about any challenges they experienced in implementing TSA's *Pipeline Security Guidelines*. Based on the results of our operator interviews, we analyzed TSA data on critical facility identification. Further, to assess TSA's process for updating the guidelines, we compared the process with TSA's *Pipeline Security Smart Practice Observations* for pipeline operators and our *Standards for Internal Control in the Federal Government*.¹³

To determine the extent TSA has assessed security risks to pipelines, we reviewed key threat assessments from TSA, such as its Pipeline Modal and Cyber Modal Threat Assessments and Transportation Sector Security Risk Assessments that it issued during calendar years 2011 through 2017. We also evaluated TSA's identification of the 100 most critical pipeline systems, its methods for assessing relative risk among those systems, and its prioritization of its pipeline reviews. As part of that evaluation, we assessed the reliability of the data within TSA's pipeline relative risk ranking tool by performing electronic and manual checks for such things as logic errors and missing data.¹⁴ Additionally, we interviewed TSA officials about how the risk tool is updated and maintained to ensure data reliability. We determined the data were sufficiently reliable for the purpose of our review. We also interviewed TSA officials about the methods they used to rank relative risk among pipeline systems and the extent to which those methods aligned with the *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (NIPP),¹⁵ other Department of Homeland Security (DHS) priorities, and previously identified best practices for program management and risk assessment. We also analyzed information on the number of pipeline security reviews—Corporate Security Reviews (CSR) and Critical Facility Security Reviews (CFSR)—that TSA conducted by Fiscal Year, as well as TSA staffing levels and contractor support. Further, we interviewed TSA officials about their staffing allocation and workforce planning process and compared TSA's process to our previous work which identified principles that a strategic workforce planning process should follow.¹⁶

To further our understanding of TSA's pipeline security review processes, we observed TSA officials and contractors conduct one CSR of one pipeline system, and three CFSRs at three critical facilities in the Houston and Beaumont, Texas, areas. While the results of our observations cannot be generalized to all CSRs and CFSRs or all pipeline systems and critical facilities, they provided us with an understanding of how TSA conducts these reviews and inspections. We also interviewed representatives of Secure Solutions International—a security and risk management consulting firm that assists TSA in conducting CSRs and CFSRs—about critical facilities and the inspection process.

To determine the extent TSA has assessed its effectiveness in reducing pipeline security risks, we assessed key strategic documents, such as TSA's performance report, against our key characteristics of effective performance measures.¹⁷ We also reviewed TSA guidance, such as the standard operating procedures outlining how TSA staff are to conduct pipeline security reviews and monitor operators' implementation of their recommendations. We then compared TSA's assessment efforts to our *Standards for Internal Control in the Federal Government*. In addition, we evaluated the databases TSA officials reported using to analyze and record the results and recommendations of pipeline security reviews. We reviewed each database to determine what information was stored in them, such as the number of observations, what fields were present, and typical entries within each field. We then reviewed and conducted electronic testing on the universe of fields and observations. Although we identified limitations, which we discuss later in the report, we found that the data was sufficiently reliable to provide general information such as summary figures describing pipeline security reviews completed. We also interviewed

¹³ GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 10, 2014).

¹⁴ To assess the security risks of the top 100 critical pipeline systems, TSA's Pipeline Security Branch developed its Pipeline Relative Risk Ranking Tool (risk assessment) in 2007. The risk assessment calculates threat, vulnerability, and consequence on variables such as the amount of throughput in the pipeline system.

¹⁵ Department of Homeland Security, *2013 National Infrastructure Protection Plan, Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: December 2013).

¹⁶ GAO, *Human Capital: Key Principles for Effective Strategic Workforce Planning*, GAO-04-39 (Washington, D.C.: Dec. 11, 2003).

¹⁷ GAO, *Tax Administration: IRS Needs to Further Refine Its Tax Filing Season Performance Measures*, GAO-03-143 (Washington, D.C.: Nov. 22, 2002); GAO, *Military Personnel: DOD Needs to Establish Performance Measures for the Armed Forces Sports Program*, GAO-17-542 (Washington, D.C.: June 8, 2017).

TSA officials to understand TSA's efforts to assess its overall effectiveness in reducing pipeline security risks and related data collection efforts.

We conducted this performance audit from June 2017 to December 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

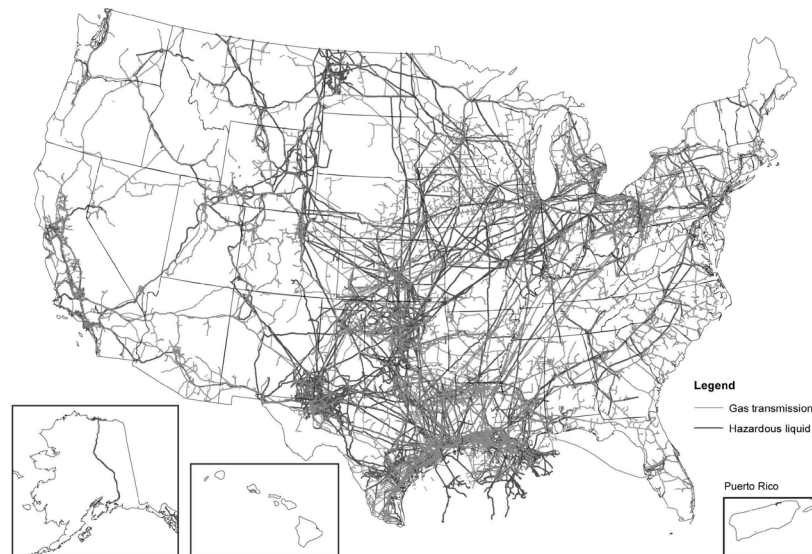
Overview of the U.S. Pipeline System

The national pipeline system consists of more than 2.7 million miles of networked pipelines transporting oil, natural gas, and other hazardous liquids. Hazardous liquid and natural gas pipelines—primarily buried underground in the continental United States—run under remote and open terrain, as well as densely populated areas. These pipelines are of three main types:

- Hazardous liquid: About 216,000 miles of hazardous liquid pipeline transport crude oil, diesel fuel, gasoline, jet fuel, anhydrous ammonia, and carbon dioxide.
- Natural gas transmission and storage: About 319,000 miles of pipeline—mostly interstate—transport natural gas from sources to communities.
- Natural gas distribution: About 2.2 million miles of pipeline—mostly intra-state—transport natural gas from transmission sites to consumers.

Figure 1 depicts the network of hazardous liquid and natural gas transmission pipelines in the United States.

Figure 1: Map of Hazardous Liquid and Natural Gas Transmission Pipelines in the United States, September 2018

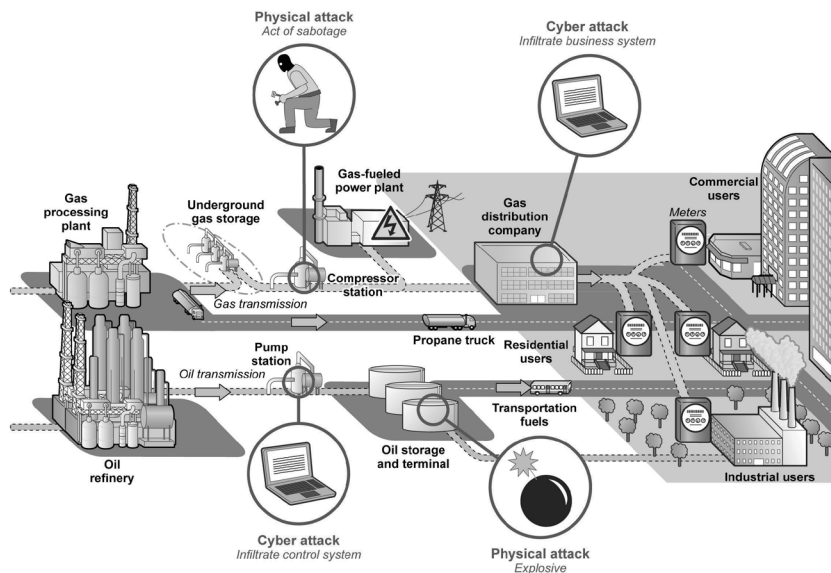


More than 3,000 pipeline companies operate the Nation's pipeline systems, which can traverse multiple states and the U.S. borders with Canada and Mexico. Many pipeline systems are comprised of the pipelines themselves, as well as a variety of facilities, such as storage tanks, compressor stations, and control centers. Most pipeline systems are monitored and moderated through automated ICS or Supervisory Control and Data Acquisition (SCADA) systems using remote sensors, signals, and preprogrammed parameters to activate and deactivate valves and pumps to maintain flows within tolerances.¹⁸

¹⁸ SCADA is one type of control system, which is a computer-based system used within many infrastructures and industries to monitor and control sensitive processes and physical functions. Control systems perform functions that range from simple to complex. They can be used to simply monitor processes—for example, the environmental conditions in a small office building—

Federal agencies and pipeline operators determine the criticality of pipeline systems and their facilities based on their importance to the Nation's energy infrastructure; service to installations critical to national defense; or, if attacked, have the potential to cause mass casualties and significant impact on public drinking water affecting major population centers. Accordingly, those determined to be critical merit increased attention to security. However, as we previously reported, the inherent design and operation of U.S. pipeline systems may reduce some potential impacts of lost service.¹⁹ The pipeline sector is generally considered to be resilient and versatile. Historically, pipeline operators have been able to quickly respond to the adverse consequences of an incident—whether it is damage from a major hurricane or a backhoe—and quickly restore pipeline service. Pipeline infrastructure also includes redundancies such as parallel pipelines or interconnections that enable operators to reroute material through the network. Figure 2 depicts the U.S. pipeline system, its basic components, examples of vulnerabilities, and the entities to which it supplies energy and raw materials. These entities include utility companies, airports, military sites, and industrial and manufacturing facilities.

Figure 2: U.S. Natural Gas and Oil Pipeline Systems' Basic Components and Examples of Vulnerabilities



Source: GAO analysis of Transportation Security Administration information. | GAO-19-48

Physical and Cyber Threats to Pipeline Systems

According to TSA, pipelines are vulnerable to physical attacks—including the use of firearms or explosives—largely due to their stationary nature, the volatility of transported products, and the dispersed nature of pipeline networks spanning urban and outlying areas. The nature of the transported commodity and the potential effect of an attack on national security, commerce, and public health make some pipelines and their assets more attractive targets for attack.²⁰ Oil and gas pipelines have been and continue to be targeted by terrorists and other malicious groups globally.²¹ Terrorists have also targeted U.S. pipelines, but have not succeeded in at-

or to manage the complex activities of a municipal water system or a nuclear power plant. Control systems are vulnerable to cyber-attack from inside and outside the control system network.

¹⁹ GAO-10-867.

²⁰ Transportation Security Administration, *Biennial National Strategy for Transportation Security: Report to Congress* (Washington, D.C.: Apr. 4, 2018).

²¹ For example, rebels bombed the Caño Limón oil pipeline and other pipelines in Colombia more than 600 times since 1993, with the most recent attack occurring on April 27, 2017. Militants in Nigeria have repeatedly attacked oil pipelines, including coordinated bombings of three pipelines in 2007 and the bombing of an underwater pipeline in 2016. Assailants bombed natural gas pipelines in British Columbia, Canada six times between October 2008 and July 2009, which authorities later classified as environmentally-motivated. See GAO-10-867 and Congress-

Continued

tacking them.²² Further, environmental activists and lone actors seeking to halt the construction of new pipelines through sabotage have recently emerged as a new threat to pipelines.²³ For example, in March 2017, activists used blowtorches to cut holes in empty portions of the Dakota Access Pipeline in two states. In February 2017, local law enforcement officers fatally shot a man who used an assault rifle to damage the Sabal Trail Pipeline, a natural gas pipeline under construction in Florida.

The sophisticated computer systems that pipeline operations rely on are also vulnerable to various cyber threats.²⁴ According to DOE, the frequency, scale, and sophistication of cyber threats have increased, and attacks have become easier to launch. NCCIC reported that the energy sector, which includes pipelines, experienced more cyber incidents than any sector from 2013 to 2015, accounting for 35 percent of the 796 incidents reported by all critical infrastructure sectors. In 2016, NCCIC reported that the energy sector was the third most frequently attacked sector.²⁵ Further, according to DOE, the cost of preventing and responding to cyber incidents in the energy sector is straining the ability of companies to adequately protect their critical cyber systems.²⁶ For example, a 2015 study by the Ponemon Institute estimated the annualized cost of cyber crime for an average energy company to be about \$28 million.²⁷

Ineffective protection of cyber assets from these threats can increase the likelihood of security incidents and cyber attacks that disrupt critical operations; lead to inappropriate access to and disclosure, modification, or destruction of sensitive information; and threaten national security, economic well-being, and public health and safety. Unintentional or nonadversarial threat sources may include failures in equipment or software due to aging, resource depletion, and errors made by end users. They also include natural disasters and failures of critical infrastructure on which the organization depends, but that are outside of the control of the organization.

Intentional or adversarial threats may include corrupt employees, criminal groups, terrorists, and nations that seek to leverage the organization's dependence on cyber resources (*i.e.*, information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies). These threat adversaries vary in terms of their capabilities, their willingness to act, and their motives, which can include seeking monetary gain or seeking an economic, political, or military advantage.

Cyber threat adversaries make use of various techniques, tactics, practices, and exploits to adversely affect an organization's computers, software, or networks, or to intercept or steal valuable or sensitive information. For example, an attacker could infiltrate a pipeline's operational systems via the Internet or other communication pathways to potentially disrupt its service and cause spills, releases, explo-

sional Research Service, *Pipelines: Securing the Veins of the American Economy*, TE10009 (Washington, D.C.: Apr. 19, 2016).

²² In 2006, Federal authorities acknowledged the discovery of a detailed posting on a website purportedly linked to al Qaeda that reportedly encouraged attacks on U.S. pipelines, especially Trans Alaska Pipeline System, using weapons or hidden explosives. In 2007, the U.S. Department of Justice arrested members of a terrorist group planning to attack jet fuel pipelines and storage tanks at the John F. Kennedy International Airport. In 2011, a man planted a bomb, which did not detonate, along a natural gas pipeline in Oklahoma. In 2012, a man unsuccessfully attempted to bomb a natural gas pipeline in Plano, Texas. See GAO-10-867 and Congressional Research Service, Testimony TE10009, *Pipelines: Securing the Veins of the American Economy*, by Paul W. Parfomak, Apr. 19, 2016.

²³ Congressional Research Service, *Pipeline Security: Recent Attacks*, IN106103 (Washington, D.C.: Apr. 11, 2017).

²⁴ Once accessible to an attacker, a SCADA system can be exploited in a number of specific ways to carry out a cyber attack: issuing unauthorized commands to control equipment; sending false information to a control-system operator that initiates inappropriate actions; 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. Congressional Research Service, *Cybersecurity for Energy Delivery Systems*, R44939 (Washington, D.C.: Aug. 28, 2017).

²⁵ NCCIC collects data on cyber incidents that attempt to gain access to both business and control systems infrastructure. These incidents, reported on a voluntary basis by critical infrastructure owners and operators, include, for example, unauthorized access to SCADA devices or exploitation of software vulnerabilities. NCCIC reports data on critical infrastructure sectors, such as energy, but does not report data on subsectors, such as pipelines.

²⁶ Department of Energy, Office of Electricity Delivery and Reliability, *Multiyear Plan for Energy Sector Cybersecurity, 2018* (Washington, D.C.: Mar. 2018).

²⁷ Ponemon Institute, *2015 Cost of Cyber Crime Study: United States*, 2016.

sions, or fires.²⁸ Moreover, ICS, which were once largely isolated from the Internet and the company's information technology systems, are increasingly connected in modern energy systems, allowing cyber attacks to originate in business systems and migrate to operational systems. For example, malicious nation-state actors used spear-phishing²⁹ and other similar approaches in 2018 against energy sector organizations to gain access to their business systems, conduct reconnaissance, and collect information about their ICS.³⁰ Similarly, in April 2012, the Industrial Control Systems Cyber Emergency Response Team reported that an unidentified cyber attacker had conducted a series of cyber intrusions into U.S. natural gas pipeline systems beginning in December 2011.³¹

Key Critical Infrastructure Protection Guidance and Presidential Directives

Federal policy and public-private plans establish roles and responsibilities for the protection of critical infrastructure, including pipelines. These include Presidential Policy Directive 21 (PPD-21), the NIPP, and Executive Order 13636. PPD-21, issued in February 2013, reflects an all-hazards approach to protecting critical infrastructure, including natural disasters, terrorism, and cyber incidents.³² The directive also identifies the 16 critical infrastructure sectors³³ and assigns roles and responsibilities for each critical infrastructure sector among nine designated Federal sector-specific agencies.³⁴

While PPD-21 identified the critical infrastructure sectors and assigned responsibility for each sector's sector-specific agency, the NIPP outlines critical infrastructure stakeholder roles and responsibilities regarding critical security and resilience. It describes a voluntary partnership model as the primary means of coordinating government and private sector efforts to protect critical infrastructure. As part of

²⁸ In 2007, researchers working with DHS conducted an experiment to prove such an attack is possible by sending two sets of commands to a diesel-fueled electric generator, which caused the generator to destroy itself without the operators knowing. In addition, according to DOE, in 2015, unidentified attackers used spear phishing e-mails to gain access to three Ukrainian utilities' information technology networks resulting in power loss for 225,000 customers for several hours. Once inside, among other things, they stole credentials and hijacked the distribution management system to systematically open breakers and cause a power outage. The attackers then accessed the industrial control system network and disabled the uninterruptible power supply, operational control systems, and computers and prevented infected computers from re-booting.

²⁹ "Spear-phishing" involves sending official-looking e-mails to specific individuals to insert harmful software programs (malware) into protected computer systems; to gain unauthorized access to proprietary business information; or to access confidential data such as passwords, social security numbers, and private account numbers.

³⁰ NCCIC and the Federal Bureau of Investigation characterized the intrusions as a multi-stage intrusion campaign by an identified nation state's actors on U.S. Government entities and organizations within the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors. According to the agencies, the campaign targeted small commercial facilities' networks where they staged malware, conducted spear phishing, and gained remote access into energy sector networks. After obtaining access, the actors conducted network reconnaissance, moved laterally, and collected information pertaining to industrial control systems. Federal Bureau of Investigation and National Cybersecurity and Communications Integration Center, Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors TA18-074A (Washington, D.C.: Mar., 16 2018 (revised)).

³¹ Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), *ICS-CERT Monthly Monitor* (Washington, D.C.: Apr. 2012).

³² White House, *Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 12, 2013). The term "all-hazards" is defined by the directive as a threat or an incident, natural or manmade, which warrants action to protect life, property, the environment, and public health or safety, and to minimize disruptions of government, social, or economic activities. "All-hazards," as further defined in the directive, includes natural disasters, cyber incidents, industrial accidents, pandemics, acts of terrorism, sabotage, and destructive criminal activity targeting critical infrastructure.

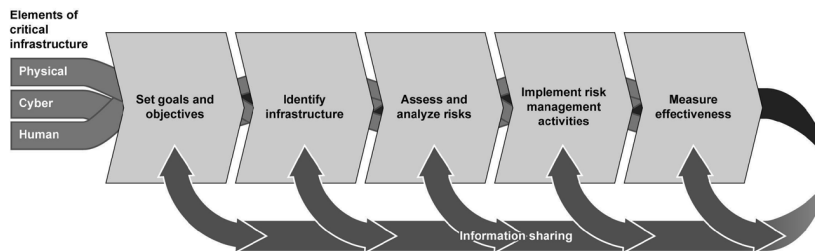
³³ The 16 critical infrastructure sectors are Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Health Care and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems; and Water and Wastewater Systems.

³⁴ PPD-21 was developed to advance a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure. It defines resilience as the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions, and includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. Stated another way, resilience can reduce the consequences associated with an incident, event, or occurrence. Resilience is an area that may be included in vulnerability assessments to determine the extent to which critical infrastructure is prepared to withstand and recover from disruptions. Such disruptions could include exposure to a given hazard or incidents arising from the deliberate exploitation of vulnerabilities of sector-specific strategies, policies, activities, and issues.

the partnership structure, the designated sector-specific agencies serve as the lead coordinators for security programs of their respective sector. As sector-specific agencies, Federal departments or agencies lead, facilitate, or support the security and resilience programs and associated activities of their designated critical infrastructure sector. For example, DHS and DOT are both designated as sector-specific agencies for the transportation systems sector, which includes pipelines. Each sector also has a government coordinating council,³⁵ consisting of representatives from various levels of government, and many have a sector coordinating council (SCC) consisting of owner-operators of these critical assets or members of their respective trade associations.³⁶ For example, the Transportation Government Coordinating Council has been established, and the Pipeline Modal SCC has been established to represent pipeline operators.³⁷

The NIPP also outlines a risk management framework for critical infrastructure protection. As shown in Figure 3, the NIPP uses a risk management framework as a planning methodology intended to inform how decision makers take actions to manage risk. The risk management framework calls for public and private critical infrastructure partners to conduct risk assessments to understand the most likely and severe incidents that could affect their operations and communities, and use this information to support planning and resource allocation.

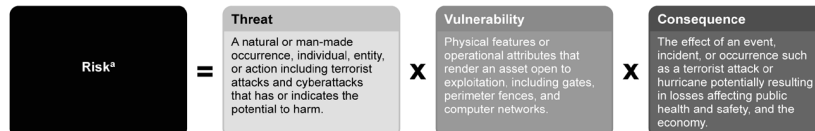
Figure 3: The National Infrastructure Protection Plan's Critical Infrastructure Risk Management Framework



Source: Department of Homeland Security National Infrastructure Protection Plan 2013. | GAO-19-48

According to DHS, the risk management framework is influenced by the nature and magnitude of a threat, the vulnerabilities to that threat, and the consequences that could result, as shown in Figure 4.

Figure 4: Determination of Risks Related to Infrastructure Protection



Source: GAO analysis of the Department of Homeland Security's National Infrastructure Protection Plans (2009 and 2013). | GAO-19-48

^a As noted in DHS's Risk Management Fundamentals Doctrine, risk is generally recognized as a function of threats, vulnerabilities, and consequences—elements that may explicitly be considered for many homeland security risks, such as those related to infrastructure protection. Risk Management Fundamentals, Homeland Security Risk Management Doctrine (Washington, D.C.: April 2011).

Federal policy has encouraged voluntary information-sharing mechanisms between the Federal government and critical infrastructure owners and operators.³⁸

³⁵ Government coordinating councils coordinate strategies, activities, policy, and communications across government entities within each sector and consist of representatives across various levels of government (*i.e.*, federal, state, local, and tribal) as appropriate. For example, DHS and DOE are designated as the co-chairs of the Energy Government Coordinating Council.

³⁶ SCCs are self-organized, self-run, and self-governed private sector councils that interact on a wide range of sector-specific strategies, policies, and activities. SCC membership can vary from sector to sector, but is meant to be representative of a broad base of owners, operators, associations, and other entities—both large and small—within the sector.

³⁷ Pipeline operators may also participate in the Oil and Natural Gas Subsector Coordinating Council of the Energy SCC.

³⁸ Among other things, Presidential Decision Directive 63, for example, encouraged the development of ISACs to serve as mechanisms for gathering, analyzing, and disseminating information on cyber infrastructure threats and vulnerabilities to and from owners and operators of the

For example, Information Sharing and Analysis Centers (ISAC) are formed by critical infrastructure owners and operators to gather, analyze, appropriately sanitize, and disseminate intelligence and information related to critical infrastructure. They typically collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency. ISACs in which pipeline operators may participate have been formed including the Oil and Natural Gas ISAC, Downstream Natural Gas ISAC, and Electricity ISAC.

Finally, in February 2013, the president issued Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, which cited repeated cyber intrusions into critical infrastructure as demonstrating the need for improved cybersecurity.³⁹ Executive Order 13636 outlined actions for improving critical infrastructure cybersecurity, including direction for the National Institute of Standards and Technology (NIST) to lead the development of a voluntary risk-based cybersecurity framework that would comprise a set of industry standards and best practices to help organizations manage cybersecurity risks.⁴⁰ NIST issued the framework in 2014 and updated it in April 2018.⁴¹ The order also addressed the need to improve cybersecurity information sharing and collaboratively develop risk-based standards and stated that U.S. policy was to increase the volume, timeliness, and quality of cyber threat information shared with private sector entities so that these entities may better protect and defend themselves against cyber threats.

Pipeline Stakeholders' Security Roles and Responsibilities

Protecting the Nation's pipeline systems is a responsibility shared by both the Federal government and private industry. As a result, several Federal departments, agencies, and the private sector have significant roles in pipeline physical and cyber-related security. These entities include the following:

Transportation Security Administration (TSA). TSA, within DHS, has primary oversight responsibility for the physical security and cybersecurity of transmission and distribution pipeline systems.⁴² Within TSA, the Security Policy and Industry Engagement's Pipeline Security Branch is charged with overseeing its pipeline security program. Pursuant to its authority, TSA's Pipeline Security Branch first issued its voluntary *Pipeline Security Guidelines* in 2011, and released revised guidelines in March 2018.⁴³ In accordance with the 9/11 Commission Act, TSA's Pipeline Security Branch identifies the top 100 critical pipeline systems in the Nation.⁴⁴ To do so, it uses system annual throughput, which is based on the amount of hazardous liquid or natural gas product transported through a pipeline in 1 year (*i.e.*, annual throughput). TSA also ranks the relative risk among the top 100 critical pipeline systems, discussed later in the report. Additionally, TSA's Pipeline Security Branch is responsible for conducting voluntary Corporate Security Reviews (CSR) and Crit-

sectors and the Federal government. White House, *Presidential Decision Directive 63: Critical Infrastructure Protection: Sector Coordinators*, (Washington, D.C.: May 22, 1998). Presidential Decision Directive 63 has been superseded by Homeland Security Policy Directive 7, which was revoked by PPD-21.

³⁹ Exec. Order No. 13636 (Feb. 12, 2013), 78 Fed. Reg. 11,737 (Feb. 19, 2013). Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, issued in May 2017, directs the Secretary of Homeland Security, in coordination with the heads of other appropriate departments and agencies, to among other things, identify authorities and capabilities that agencies could use to support the cybersecurity efforts of critical infrastructure entities identified pursuant to section 9 of Executive Order 13636 to be at greatest risk of attack that could result in catastrophic results on public health or safety, economic security, or national security. See Exec. Order No. 13800 (May 11, 2017), 82 Fed. Reg. 22,391 (May 16, 2017).

⁴⁰ Exec. Order No. 13636, 78 Fed. Reg. at 11,740-41. The National Institute of Standards and Technology (NIST) is a standards-setting agency under the U.S. Department of Commerce.

⁴¹ National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014); *Framework for Improving Critical Infrastructure Cybersecurity* Version 1.1 (Apr. 16, 2018).

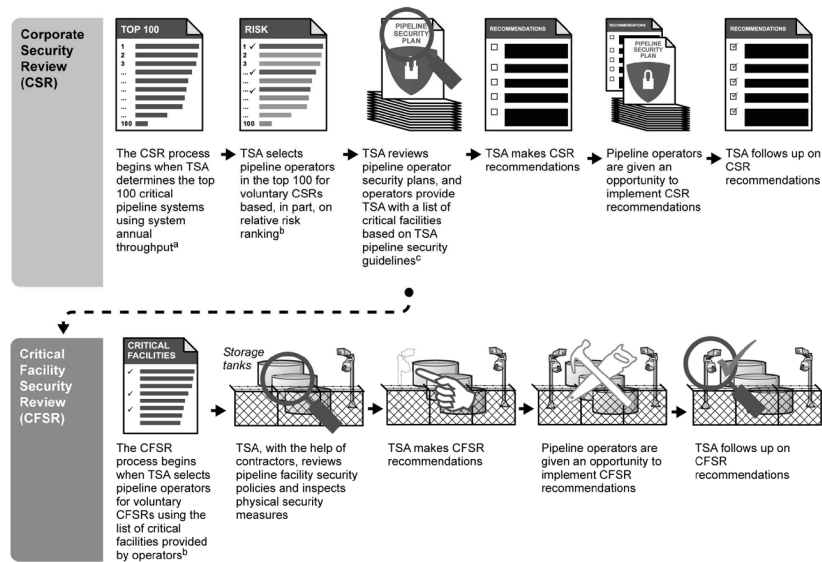
⁴² Pursuant to the Aviation and Transportation Security Act, TSA is the Federal entity with responsibility for security in all modes of transportation, which includes the Nation's interstate pipeline systems. See Pub. L. No. 107-71, 115 Stat. 597 (2001); 49 U.S.C. § 114(d).

⁴³ The Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act) directs the Secretary of Homeland Security, in conjunction with the Secretary of Transportation, to develop and transmit to pipeline operators security recommendations for natural gas and hazardous liquid pipelines and pipeline facilities and, if deemed appropriate, shall promulgate regulations and carry out necessary inspection and enforcement actions. See Pub. L. No. 110-53, § 1557(d), 121 Stat. 266, 475-76; 6 U.S.C. § 1207(d). TSA has not issued regulations for the pipeline sector under this authority but instead relies on voluntary compliance with the agency's security guidelines and best practice recommendations.

⁴⁴ See 6 U.S.C. § 1207(b). According to Pipeline Security Branch officials, even though there are over 3,000 pipeline operators in the U.S., the top 100 critical pipeline systems in the country represent approximately 85 percent of the energy in the Nation.

ical Facility Security Reviews (CFSR), which assess the extent to which the 100 most critical pipeline systems are following the intent of TSA's *Pipeline Security Guidelines*.⁴⁵ See figure 5 below for an overview of the CSR and CFSR processes.

Figure 5: Overview of the Transportation Security Administration's (TSA) Voluntary Security Review Processes with Pipeline Operators



Source: GAO analysis of TSA information. | GAO-19-48

^aTSA uses system annual throughput in determining the top 100 critical pipeline system, which is based on the amount of hazardous liquid or natural gas product transported through a pipeline in 1 year (*i.e.*, annual throughput measured in therms). Also, some pipeline operators own or operate more than one of the 100 most critical systems.

^bBecause of the voluntary nature of TSA's pipeline security program, TSA requests selected operators to participate in its pipeline security reviews—the CSR and CFSR. An operator may choose not to participate in these reviews. However, according to TSA officials, no operator has declined to participate in a CSR or CFSR to date.

^cUnder TSA's Pipeline Security Guidelines, pipeline operators are to self-identify the critical facilities within their pipeline system and report their critical facilities to TSA. However, operators may identify no critical facilities in their systems.

In addition, TSA Intelligence and Analysis is responsible for collecting and analyzing threat information related to the transportation network, and sharing relevant threat information to pipeline stakeholders.

National Cybersecurity and Communications Integration Center (NCCIC). Within DHS, NCCIC assists critical infrastructure owners in addressing cyber incidents and attacks, including those targeting industrial control systems.⁴⁶ The NCCIC's mission is to reduce the likelihood and severity of incidents that may significantly compromise the security and resilience of the Nation's critical information technology and communications networks.⁴⁷ NCCIC's role is to serve as the Federal civilian interface for sharing information related to cybersecurity risks, incidents, analysis, and warnings with Federal and nonfederal entities, and to provide shared

⁴⁵ CSRs are voluntary on-site reviews of a pipeline owner's corporate policies and procedures. CFSRs are voluntary onsite reviews of critical pipeline facilities, as well as other selected pipeline facilities throughout the Nation. TSA requests selected operators to participate in these reviews, but operators can decline to participate. However, according to TSA officials, no operator has declined to participate in a CSR or CFSR.

⁴⁶ According to NCCIC officials, NCCIC is in the process of an organizational realignment. When completed, the United States Cyber Emergency Team and the Industrial Control Systems Cyber Emergency Team will be consolidated into a single entity within NCCIC.

⁴⁷ National Security Presidential Directive 54 (Homeland Security Presidential Directive/HSPD-23), issued on January 8, 2008, established the Comprehensive National Cybersecurity Initiative, which is aimed at safeguarding Federal civilian Executive Branch government information systems. Pursuant to the directive, DHS established the NCCIC in October 2009.

situational awareness to enable real-time actions to address cybersecurity risks and incidents to Federal and nonfederal entities.

Pipeline and Hazardous Materials Safety Administration (PHMSA). PHMSA, within DOT, is responsible for regulating the safety of hazardous materials transportation and the safety of pipeline systems, some aspects of which can be related to pipeline security.⁴⁸ In 2004, PHMSA and TSA entered into a memorandum of understanding regarding their respective roles in all modes of transportation. In 2006, they signed an annex to the memorandum of understanding that further delineates lines of authority and responsibility between TSA and PHMSA on pipeline and hazardous materials transportation security. The annex identifies TSA as the lead Federal entity for transportation security, including hazardous materials and pipeline security, and PHMSA as responsible for administering a national program of safety in natural gas and hazardous liquid pipeline transportation, including identifying pipeline safety concerns and developing uniform safety standards.

Department of Energy (DOE). DOE is responsible for protecting electric power, oil, and natural gas delivery infrastructure and, in December 2015, was identified in statute as the sector-specific agency for cybersecurity for the energy sector.⁴⁹ The Office of Cybersecurity, Energy Security, and Emergency Response is the lead for DOE's cybersecurity efforts.⁵⁰ In addition, DOE operates the National SCADA Test Bed Program, a partnership with Idaho National Laboratory, Sandia National Laboratories, and other national laboratories which addresses control system security challenges in the energy sector. Among its key functions, the program performs control systems testing, research, and development; control systems requirements development; and industry outreach.

Federal Energy Regulatory Commission (FERC). FERC regulates the U.S. bulk electric power system, which is increasingly powered by natural gas pipeline systems.⁵¹ FERC has regulatory authority over interstate natural gas pipelines under the Natural Gas Act.⁵² However, its role is limited to natural gas pipeline siting and rate regulation. The North American Electric Reliability Corporation is the federally designated U.S. Electric Reliability Organization, and is overseen by FERC. The North American Electric Reliability Corporation, with approval from FERC, has developed mandatory critical infrastructure protection standards for protecting electric utility-critical and cyber-critical assets.

Private sector. Although TSA has primary Federal responsibility for overseeing interstate pipeline security, private sector pipeline operators are responsible for implementing asset-specific protective security measures. As we previously reported, operators have increased their attention on security by incorporating security practices and programs into their overall business operations.⁵³ Pipeline operators' interests and concerns are primarily represented by five major trade associations with ties to the pipeline industry—the Interstate Natural Gas Association of America (INGAA), American Gas Association (AGA), American Public Gas Association, American Petroleum Institute (API), and Association of Oil Pipe Lines. According to TSA officials, pipeline operators, and association representatives, these associations have worked closely with the Federal government on a variety of pipeline security-related issues, including collaborating on TSA's voluntary standards and information sharing.

Federal and Nonfederal Pipeline Stakeholders Exchange Risk-Related Security Information

All of the pipeline operators and pipeline association representatives we interviewed reported receiving security information from Federal and nonfederal entities. Pipeline operators also reported providing security-related information to Federal

⁴⁸The Homeland Security Act of 2002, enacted in November 2002, established DHS, transferred TSA from DOT to DHS, and assigned DHS responsibility for protecting the Nation from terrorism, which includes securing the Nation's transportation systems. See Pub. L. No. 107-296, 116 Stat. 2135 (2002). Primary responsibility for regulating the safety of hazardous materials transportation via pipeline and the safety of pipeline systems remained with DOT. See *e.g.*, 49 C.F.R. pts. 190–199.

⁴⁹See Pub. L. No. 114–94, § 61003(c)(2), 129 Stat. 1312, 1779 (2015).

⁵⁰DOE's Office of Cybersecurity, Energy Security and Emergency Response cybersecurity program for energy delivery systems is structured around three areas: (1) cybersecurity preparedness; (2) cyber incident response and recovery; and (3) research, development, and demonstration.

⁵¹FERC approved mandatory and enforceable cybersecurity standards in 2008 and physical security standards in 2014 for U.S. bulk electric operators. See 73 Fed. Reg. 7,368 (Feb. 7, 2008) (Order No. 706), 79 Fed. Reg. 70,069 (Nov. 25, 2014) (Order No. 802); see also 18 C.F.R. pt. 40.

⁵²See 42 U.S.C. § 7172.

⁵³GAO–10–867.

agencies, including TSA, as incidents occur. Multiple Federal entities exchange alerts of physical and cybersecurity incidents and other risk-related information with critical infrastructure partners, including pipeline operators. For example, DHS components including TSA's Intelligence and Analysis and NCCIC share security-related information on physical and cyber threats and incidents with sector stakeholders. Specifically, Intelligence and Analysis provides quarterly intelligence briefings to pipeline operators. NCCIC also issues indicator bulletins, which can contain information related to cyber threat indicators, defensive measures, and cybersecurity risks and incidents.

In addition, TSA and other Federal entities have coordinated to address specific pipeline-related security incidents. For example, TSA officials coordinated with DOT, DOE, the Department of Justice, and FERC through the Oil and Natural Gas subsector SCC to address ongoing incidents of vandalism and sabotage of critical pipeline assets by environmental activists in 2016. In July 2017, according to DOT officials, PHMSA and TSA collaborated on a web-based portal to facilitate sharing sensitive but unclassified incident information among Federal agencies with pipeline-related responsibilities. See table 1 for the key Federal information sharing entities and programs that exchange security-related or incident information with critical infrastructure stakeholders, including the pipeline sector.

Table 1: Federal Information Sharing Entities and Programs that Provide Information to Pipeline Stakeholders

Entity/Program	Product/service description
<i>Department of Homeland Security (DHS)</i>	
<i>National Cybersecurity and Communications Integration Center (NCCIC)</i>	NCCIC receives, triages, tracks, coordinates, and manages high volumes of threat, vulnerability, and incident information on a 24/7 basis. The watch floor disseminates this information to NCCIC analysts for resolution and shares alerts, reports, and other information products with the pipeline community. NCCIC also facilitates weekly teleconferences with private and public entities to discuss situational awareness and provide ongoing informational analysis related to current events. In addition, its Cyber Information Sharing and Collaboration Program bulletins provide incident analysis information derived from new cyber incidents or malicious code, threats, and vulnerabilities to, among others, pipeline operators. ^a
<i>Transportation Security Administration (TSA)</i> <i>Transportation Security Operations Center (TSOC)</i>	The TSOC is the conduit with which TSA coordinates with DHS, the Federal Aviation Administration, the Federal Bureau of Investigation, and other law enforcement and security agencies to analyze and monitor security-related operations, incidents and crises in all transportation modes. In addition, pipeline operators are asked to voluntarily report security incidents to TSA via the TSOC.
<i>TSA Intelligence and Analysis</i>	Intelligence and Analysis is to provide pipeline industry security professionals with timely and actionable information on terrorist threats to hazardous liquid and natural gas pipelines. For example, Intelligence and Analysis is to prepare quarterly and annual pipeline cyber and physical modal threat assessments and unclassified quarterly threat briefings based on analysis of primary threat actors, credible terrorist plots, and successful attacks, as well as tactics, techniques, procedures, and targets that could be employed in future attacks.
<i>National Terrorism Advisory System (NTAS)</i>	NTAS Bulletins—NTAS, DHS's system for communicating terrorist threats to the American public, issues bulletins that communicate terrorism information alerting sector stakeholders, including pipeline owners/operators, of any elevated (<i>i.e.</i> , general information about timing and target) or imminent (<i>i.e.</i> , credible, specific, and impending) threats.
<i>Homeland Security Information Network (HSIN)</i>	HSIN is the trusted network for homeland security mission operations to share sensitive but unclassified information. Federal, state, local, territorial, tribal, international, and private sector homeland security partners are to use HSIN to manage operations, analyze data, and send alerts and notices of cyber and physical security threats.
<i>Protective Security Advisor (PSA) Program</i>	PSAs are security subject matter experts who engage with state, local, tribal, and territorial government mission partners and members of the private sector stakeholder community to protect the Nation's critical infrastructure. PSAs are to conduct voluntary, nonregulatory security surveys and assessments on critical infrastructure assets and facilities within their respective regions. PSAs also may conduct outreach activities with critical infrastructure owners and operators in support of DHS's infrastructure protection priorities.

Table 1: Federal Information Sharing Entities and Programs that Provide Information to Pipeline Stakeholders—Continued

Entity/Program	Product/service description
<i>Department of Transportation (DOT)</i>	
<i>Pipeline and Hazardous Materials Safety Administration (PHMSA)</i>	PHMSA issues advisory bulletins to communicate safety-related conditions to pipeline operators and can issue advisory bulletins in coordination with TSA to notify pipeline operators of a security incident including identifying the affected operators, describing the threat, and providing information on Federal resources for assistance. For example, in response to physical intrusions of pipelines and a coordinated campaign by domestic saboteurs, PHMSA issued an advisory bulletin, in coordination with TSA, to remind pipeline operators of the importance of safeguarding and securing their pipelines from physical and cyber intrusion or attack.
<i>Department of Energy (DOE)</i>	
<i>Cybersecurity Risk Information Sharing Program (CRISP)</i>	CRISP is a public-private partnership to facilitate the timely sharing of cyber threat information and develop situational awareness tools to enhance the ability of the electricity sector, including electric companies or utilities that also own a natural gas pipeline(s), to identify, prioritize, and coordinate the protection of its critical infrastructure. DOE shares actionable cyber threat information with CRISP participants in near-real time via the Electricity ISAC.
<i>Federal Energy Regulatory Commission (FERC)</i>	
<i>Office of Energy Infrastructure Security (OEIS)</i>	OEIS conducts joint voluntary assessments of natural gas pipeline entities' information and operational technology systems and networks to assess their vulnerabilities to current threats and emerging exploits. According to FERC, under its Cybersecurity Architecture Assessment program, OEIS and TSA take a collaborative, nonregulatory approach to promote secure and resilient infrastructure through the sharing of information and best practices. The goal of the assessment program is to allow the assessed entity to gain a comprehensive understanding of its overall cybersecurity posture, identify potential areas of concern, articulate actionable recommendations and observations, and identify best practices that promote improvements to the security posture of the assessed entity.

Source: GAO analysis of agency documents | GAO-19-48

*NCCIC sends Cyber Information Sharing and Collaboration Program bulletins generally to local and state government, critical infrastructure, private industry, or another country's computer emergency response team.

Pipeline operators also share security-related information with TSA and the NCCIC. In its *Pipeline Security Guidelines*, TSA requests that pipeline operators report by telephone or e-mail to its Transportation Security Operations Center (TSOC) any physical security incidents that are indicative of a deliberate attempt to disrupt pipeline operations or activities that could be considered precursors to such an attempt.⁵⁴ TSA's *Pipeline Security Guidelines* also request that operators report any actual or suspected cyber attacks that could impact pipeline industrial control systems or other information technology-based systems to the NCCIC. According to the TSOC's operating procedures, if a reported incident meets certain criteria, such as the incident was intended to or resulted in damage or requires a general evacuation of a facility, the TSOC watch officer is then to contact Office of Security and Industry Engagement officials. According to TSA officials, the TSOC does not conduct investigations of the specific security incidents that pipeline operators report. However, TSOC staff do analyze the incident information they receive for national trends and common threats. TSA officials stated that they share their observations with pipeline operators and other critical infrastructure asset owners during monthly and quarterly conference calls that TSA holds with pipeline operators.

All the pipeline operators and association representatives we interviewed identified other nonfederal information sharing entities, including ISACs, fusion centers, industry associations, and SCCs, which provide forums for exchanging information about physical and cyber incidents throughout the pipeline sector. See table 2 for nonfederal information sharing entities identified as available to pipeline operators.

⁵⁴ According to TSA officials, freight and passenger rail are the only two surface transportation modes whose operators are required to report incidents, potential threats, or significant security concerns. See 49 C.F.R. §§ 1580.105, 1580.203.

Table 2: Nonfederal Information Sharing Entities

Entity	Product/service description
<i>Downstream Natural Gas Information Sharing and Analysis Center (ISAC)</i>	The Downstream Natural Gas ISAC serves natural gas utility (distribution) and pipeline (transmission) companies by facilitating communications between participants, the Federal government, and other critical infrastructure. This ISAC is to disseminate threat information and indicators from government and other sources and provide analysis, coordination, and summarization of related industry-affecting information.
<i>Oil and Natural Gas ISAC</i>	The Oil and Natural Gas ISAC provides cyber threat information for the oil and natural gas industry. Its main goal is to assist in increasing the security posture of the industry's exploration and production, transportation, refining, and delivery systems from cyber-attacks through the analysis and sharing of cyber intelligence. As an industry owned and operated organization, it provides a mechanism for members to share information anonymously across its membership.
<i>Fusion centers</i>	Fusion centers are a collaborative effort of two or more federal, state, local, or tribal government agencies that combine resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity. For example, according to TSA officials, the New York State Intelligence Center shares threat data with pipeline operators.
<i>Industry associations</i>	Industry associations, such as the American Gas Association, the American Petroleum Institute, and the Interstate Natural Gas Association of America, representing companies delivering natural gas, exchange security-related information. Examples of such activities can include disseminating alerts from the National Cybersecurity and Communications Integration Center to their membership, hosting events to promote security awareness, and sharing security-related resources and guidance.
<i>InfraGard</i>	InfraGard, a partnership between the Federal Bureau of Investigation and the private sector, is to provide a vehicle for the timely exchange of information and promotes learning opportunities relevant to the protection of the Nation's critical infrastructure.
<i>Oil and Natural Gas Subsector Coordinating Council (SCC)</i>	The Oil and Natural Gas SCC is to provide a private forum for coordination of oil and natural gas security strategies and activities, policy, and communication across the sector to support the Nation's homeland security mission. This SCC provides a venue for industry owners and operators to mutually plan, implement, and execute sufficient and appropriate sector-wide security programs, procedures and processes, exchange information, and assess accomplishments and progress toward continuous improvement in the protection of the sector's critical infrastructure.

Source: GAO analysis of agency documents | GAO-19-48

Operators and TSA officials reported that the current backlog in granting security clearances for some key pipeline operator employees was a significant factor affecting information sharing between TSA and pipeline operators. TSA officials acknowledged that some pipeline operators have had difficulty obtaining security clearances for key employees due to ongoing backlogs in processing requests by the Office of Personnel Management National Background Investigation Bureau, and that TSA's ability to share timely information with operators whose staff do not have a clearance may be hindered. Three of the 10 pipeline operators we interviewed identified receiving timely classified security information as a specific challenge due, in part, to difficulties staff have had obtaining security clearances. Further, 7 of the 10 pipeline operators that we interviewed reported experiencing delays in obtaining a security clearance or were aware of others who had experienced this issue. However, according to three operators we interviewed, TSA was helpful in facilitating approval of security clearances for the operators' personnel to access classified information when necessary.

This security clearance challenge is not faced by pipeline operators alone. In January 2018, we designated the backlog of investigations for the clearance process and the government-wide personnel security clearance process as a high-risk area. We will continue to monitor agencies' progress in reducing the backlog and improving the security clearance process.⁵⁵

⁵⁵ See GAO press release "GAO Adds Government-wide Personnel Security Clearance Process to 'High Risk List'" (Washington, D.C., Jan. 25, 2018).

Pipeline Operators Use a Range of Guidelines and Standards to Address Risks, but TSA's Guidelines Lack Clear Definitions and a Process for Updating Them

Pipeline operators that we interviewed reported using a range of guidelines and standards to address their physical and cybersecurity risks, and all of them reported implementing TSA's voluntary *Pipeline Security Guidelines* that were applicable to their operations. TSA revised and issued its *Pipeline Security Guidelines* in March 2018, but the revised guidelines lack a defined process to consider updates to supporting guidance such as to the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework). Furthermore, TSA has not clearly defined the terms within the criteria that pipeline operators are to use to determine the criticality of their facilities.

Pipeline Operators Use a Range of Guidelines and Standards to Address Security

Pipeline operators that we interviewed reported using a range of guidelines and standards to address their physical and cybersecurity risks. For example, all 10 of the pipeline operators we interviewed stated they had implemented the voluntary 2011 TSA Pipeline Security Guidelines the operators determined to be applicable to their operations.⁵⁶ The guidelines provide TSA's recommendations for pipeline industry security practices such as establishing a corporate security program and identifying critical facilities among others (see sidebar).⁵⁷ Five of the 10 pipeline operators we interviewed characterized the guidelines as generally or somewhat effective in helping to secure their operations, 1 was neutral on their effectiveness, and 4 did not provide an assessment of the guidelines' effectiveness. However, one operator pointed out that they had not adopted the guidelines' recommended interval of 36 months or less for conducting security vulnerability assessments due to staffing limitations.⁵⁸ Also, another pipeline operator noted that they were working to implement the guidelines in the operations of a newly acquired asset that they determined was not using the guidelines in the same manner as their company.

All of the pipeline operators we interviewed reported using other guidelines or standards to address pipeline systems' security risks. For example, pipeline operators reported using and industry association representatives reported that their members use INGAA's *Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry*,⁵⁹ API's Pipeline SCADA Security standard,⁶⁰ and the NIST Cybersecurity Framework as sources of cybersecurity standards, guidelines, and practices that may be scaled and applied to address a pipeline operator's cybersecurity risks.⁶¹

⁵⁶Transportation Security Administration, *Pipeline Security Guidelines* (April 2011). TSA did not issue the revised guidelines until March 2018.

⁵⁷According to industry association officials, AGA and INGAA members have made voluntary commitments to implement TSA's *Pipeline Security Guidelines*.

⁵⁸TSA's *Pipeline Security Guidelines* call for pipeline operators of critical facilities to conduct a security vulnerability assessment or the equivalent on a periodic basis, not to exceed 36 months, and within 12 months after completion of a significant enhancement or modification to the facility.

⁵⁹Interstate Natural Gas Association of America, *Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry Version 1.3* (Washington, D.C.: September 17, 2015).

⁶⁰American Petroleum Institute, *Pipeline SCADA Security*, API Standard 1164 (June 2009).

⁶¹NIST, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0* (Feb. 12, 2014). In response to Executive Order 13636, NIST issued the *Framework for Critical Infrastructure Cybersecurity*, which is intended to help organizations apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. The framework consists of five concurrent and continuous functions—identify, protect, detect, respond, and recover. When considered together, these functions provide a high-level, strategic view of the life-cycle of an organization's management of cybersecurity risk.

Transportation Security Administration's *Pipeline Security Guidelines*

The Guidelines address the following areas:

1. Corporate Security Program
2. Corporate Security Plan
 - a. Security Plan Elements
3. Risk Analysis
 - a. Criticality Assessment
 - b. Security Vulnerability Assessment
4. Criticality
 - a. Facility Criticality
5. Facility Security Measures
 - a. Baseline and Enhanced Security Measures
 - b. Site-Specific Security Measures
6. Pipeline Cyber Asset Security Measures
 - a. Pipeline Cyber Assets Identification
 - b. Security Measures for Pipeline Cyber Assets
 - c. Cyber Security Planning and Implementation Guidance
7. Protective Measures for National Terrorism Advisory System Alerts

Source: Transportation Security Administration's *Pipeline Security Guidelines*, 2018. | GAO-19-48

Further, pipeline operators are required to adhere to regulations related to pipeline safety and, depending upon their assets, operations, and location, may be required to adhere to regulations for electrical utilities, chemical storage facilities, and locations near waterways. For example, all pipeline operators must adhere to DOT's PHMSA safety regulations.⁶² In addition, pipeline operators whose systems include chemical facilities may be required to comply with DHS's Chemical Facility Anti-

⁶² See 49 C.F.R. pts. 190–199.

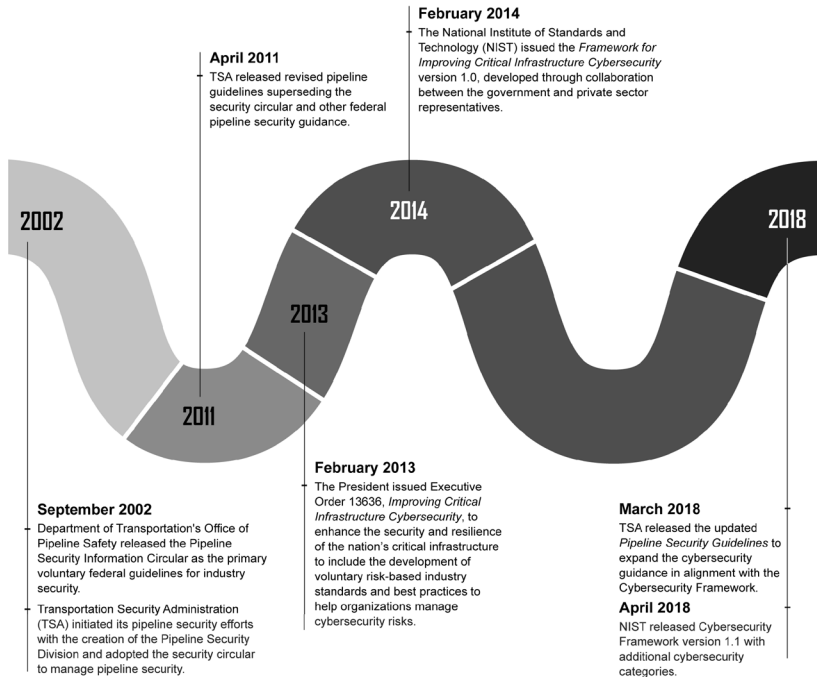
Terrorism Standards (CFATS).⁶³ Pipeline operators whose systems include a terminal located on a U.S. port may be required to comply with Maritime Transportation Security Act regulations.⁶⁴ For a listing of Federal and industry guidelines identified as applicable to security by the pipeline operators, see appendix I.

TSA Does Not Have a Documented Process for Updating Its *Pipeline Security Guidelines* to Reflect Revisions to Supporting Standards

TSA's Pipeline Security Branch issued its revised *Pipeline Security Guidelines* in March 2018, but TSA has not established a documented process to ensure that revisions occur and fully capture updates to supporting standards and guidance. The guidelines were revised to, among other things, reflect the dynamic threat environment and to incorporate cybersecurity principles and practices from the NIST Cybersecurity Framework, which were initially issued in February 2014. To revise the guidelines and incorporate feedback, according to Pipeline Security Branch officials, they incorporated outcomes from pipeline modal threat assessments and best practices from security reviews, and collaborated with pipeline sector stakeholders—including industry associations and other Federal agencies with a role in pipeline security.

Officials from the industry associations we interviewed confirmed that they provided input to the revised pipeline guidelines, including meeting with and consolidating comments from member pipeline operators. See figure 6 for a timeline of events pertinent to Federal pipeline security guidelines.

Figure 6: Timeline of Federal Pipeline Security Guidelines Development



Source: GAO analysis of NIST and TSA documents. | GAO-19-48

⁶³ See 6 C.F.R. pt. 27. In 2007, DHS established the CFATS program to assess the risk posed by chemical facilities, place High Risk facilities in one of four risk-based tiers, require High Risk facilities to develop security plans, review these plans, and inspect the facilities to ensure compliance with regulatory requirements.

⁶⁴ Maritime Transportation Security Act of 2002, enacted to protect the Nation's ports and waterways from a terrorist attack, regulates operators, including pipeline operators, with off shore or port facilities and requires certain protective measures such as vulnerability assessments and security plans. See generally Pub. L. No. 107-295, 116 Stat. 2064.

TSA's *Pipeline Security Smart Practice Observations* for pipeline operators states that security plans should have a documented process to include security plan reviews and updates on a periodic and an as-needed basis.⁶⁵ *Standards for Internal Control in the Federal Government* states that periodic review of policies, procedures, and related control activities should occur to determine their continued relevance and effectiveness in achieving identified objectives or addressing related risks.⁶⁶ The NIPP and NIST also emphasize the need to provide updates on incident response guidance and security procedures, respectively. Moreover, other pipeline industry guidance cited by TSA's guidelines also has a prescribed interval for review and revision. For example, API reviews its standards at least every 5 years.

However, TSA has not instituted a documented process to consider the need to update the *Pipeline Security Guidelines* on a regular basis. Pipeline Security Branch officials acknowledged the value of having a defined process for reviewing and, if necessary, revising TSA's *Pipeline Security Guidelines* at regular defined intervals to ensure it includes, among other things, newly identified best practices and updated industry guidance that are relevant to pipeline operators, such as the elements of the latest version of NIST's Cybersecurity Framework. For example, TSA's revisions to its guidelines incorporated some, but not all of the elements of the NIST Cybersecurity Framework version 1. Specifically, to improve incident response, the NIST framework recommends implementing an incident response analysis and feedback function to a security program. However, TSA's *Pipeline Security Guidelines* do not include similar steps for pipelines operators to include in their pipeline security programs. Further, because NIST released version 1.1 of the Cybersecurity Framework in April 2018, the guidelines that TSA released in March 2018 do not incorporate cybersecurity elements that NIST added to the latest Cybersecurity Framework such as the Supply Chain Risk Management category.⁶⁷

Pipeline Security Branch officials said that they have not instituted a review process on a regular basis because they intended to review and revise TSA's guidelines on an as-needed basis in response to updated supporting guidance, but could provide no timeline for doing so. Without a documented process defining how frequently Pipeline Security Branch staff are to review and revise its guidelines, TSA cannot ensure that its guidelines reflect the latest known standards and best practices for physical and cybersecurity, or address the persistent and dynamic security threat environment currently facing the Nation's pipeline system.

Pipeline Security Guidelines Lack Clear Definitions to Ensure Pipeline Operators Consistently Apply TSA's Criteria for Identifying Critical Facilities

Under TSA's *Pipeline Security Guidelines*, pipeline operators are to self-identify the critical facilities within their system and report their critical facilities to TSA. TSA's Pipeline Security Branch conducts CFSRs at the critical facilities that pipeline operators have identified.

However, our analysis of TSA's data found that at least 34 of the top 100 critical pipeline systems deemed highest risk indicated that they had no critical facilities.⁶⁸ Accordingly, TSA would not conduct a CFSR at any of these systems' facilities because their operators identified none of them as critical.

The fact that pipeline operators of about one third of the highest risk systems identified no critical facilities may be due, in part, to the Pipeline Security Branch not clearly defining the criteria outlined in the *Pipeline Security Guidelines* that pipeline operators are to use to determine the criticality of their facilities. Three of the 10 operators we interviewed stated that some companies reported to TSA that they had no critical facilities, and may possibly be taking advantage of the guidelines' lack of clarity. Accordingly, operators that report no critical facilities would avoid TSA's reviews of their facilities.

Our review of the eight criteria included in TSA's *Pipeline Security Guidelines* (see sidebar) found that no additional examples or clarification are provided to help operators determine criticality. Although we previously noted that 5 of the 10 opera-

⁶⁵Transportation Security Administration, *Pipeline Security Smart Practice Observations* (September 19, 2011).

⁶⁶GAO-14-704G.

⁶⁷NIST Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (April 2015). Supply chains begin with the sourcing of products and services and extend from the design, development, manufacturing, processing, handling, and delivery of products and services to the end user. Cyber supply chain risk management entails identifying, assessing, and mitigating "products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the cyber supply chain."

⁶⁸Data on critical facility count for 10 of the 100 most critical pipeline systems were not present in the ranking.

tors we interviewed generally found TSA's *Guidelines* as a whole helpful in addressing pipeline security, more than half of the operators we interviewed identified TSA's criticality criteria as a specific area for improvement. Specifically, 3 of the 10 pipeline operators that we interviewed stated that TSA had not clearly defined certain terms within the criteria, and 3 additional operators of the 10 reported that additional consultation with TSA was necessary to appropriately apply the criteria and determine their facilities' criticality. For example, 2 operators told us that individual operators may interpret TSA's criterion, "cause mass casualties or significant health effect," differently.

One of these operators that we interviewed stated that this criterion could be interpreted either as a specific number of people affected or a sufficient volume to overwhelm a local health department, which could vary depending on the locality. Another operator reported that because TSA's criteria were not clear, they created their own criteria which helped the operator identify two additional critical facilities.

**Transportation Security Administration's
Criteria for Determining Pipeline Facility
Criticality**

A facility or combination of facilities that, if damaged or destroyed, would have the potential to:

- Disrupt or significantly reduce required service or deliverability to installations identified as critical to national defense;
- Disrupt or significantly reduce required service or deliverability to key infrastructure (such as power plants or major airports) resulting in major economic disruption;
- Cause mass casualties or significant health effects;
- Disrupt or significantly reduce required service or deliverability resulting in a state or local government's inability to provide essential public services and emergency response for an extended period of time;
- Significantly damage or destroy national landmarks or monuments;
- Disrupt or significantly reduce the intended use of major rivers, lakes, or waterways (e.g., public drinking water for large populations or disruption of major commerce or public transportation routes);
- Disrupt or significantly reduce required service or deliverability to a significant number of customers or individuals for an extended period of time;
- Significantly disrupt pipeline system operations for an extended period of time (i.e., business critical facilities).

Source: Transportation Security Administration's Pipeline Security Guidelines, 2018. | GAO-19-48

Pipeline Security Branch officials acknowledged there are companies that report having no critical facilities in their pipeline systems. According to Pipeline Security Branch officials, pipeline operators are in the best position to determine which of their facilities are critical, and the companies that have determined that their pipeline systems have no critical facilities also have reported sufficient redundancies to make none of their facilities critical to the continuity of their operations. According to these officials, they have had extensive discussions with pipeline company officials to assess the validity of their criticality determinations, and have closely questioned companies to ensure they have properly applied TSA's criteria.

However, according to TSA's *Pipeline Security Guidelines*, operators should use a consistent set of criteria for determining the criticality of their facilities. In addition, *Standards for Internal Control in the Federal Government* states that management

should define objectives clearly to enable the identification of risks.⁶⁹ To achieve this, management generally defines objectives in specific and measurable terms and ensures the terms are fully and clearly set forth so they can be easily understood.

Pipeline Security Branch officials acknowledged that the criticality definitions in the *Pipeline Security Guidelines* could be clarified to be more specific. Additionally, an industry association representative reported that the association, in consultation with TSA, has been developing supplementary guidance for its members to clarify certain terms in TSA's critical facility criteria. As of October 2018 this guidance is still under review at the association and has not been made available to the association's members. Pipeline Security Branch officials confirmed they worked with the industry association on its supplementary guidance, but also acknowledged that the supplementary guidance may only be distributed to the association's membership.

Without clearly defined criteria for determining pipeline facilities' criticality, TSA cannot ensure that pipeline operators are applying its guidance uniformly. Further, because TSA selects the pipeline facilities on which to conduct CFSRs based on operators' determinations, TSA cannot fully ensure that all of the critical facilities across the pipeline sector have been identified using the same criteria, or that their vulnerabilities have been identified and addressed.

TSA Assesses Pipeline Risk and Conducts Security Reviews, but Limited Workforce Planning and Shortfalls in Assessing Risk Present Challenges

TSA's Intelligence and Analysis identifies security risks to pipeline systems through various assessments. Additionally, TSA's Pipeline Security Branch conducts security reviews to assess pipeline operators' implementation of TSA's *Pipeline Security Guidelines*, but gaps in staffing and lack of a workforce plan may affect its ability to carry out effective reviews. The Pipeline Security Branch also developed a pipeline risk assessment to rank relative risk of the top 100 critical pipeline systems and to prioritize its security reviews of pipeline companies, but shortfalls in its calculations of threat, vulnerability, and consequence may limit its ability to accurately identify pipeline systems with the highest risk. Finally, the pipeline risk assessment has not been peer reviewed to validate the assessment's data and methodology, which we previously reported as a best practice in risk management.

TSA Conducts Assessments of Pipeline Security Risks

TSA's Intelligence and Analysis produces assessments related to pipeline security risks, including Pipeline Modal and Cyber Modal Threat Assessments and the Transportation Sector Security Risk Assessment. The Pipeline and Cyber Modal Threat Assessments are issued on a semiannual basis; TSA Intelligence and Analysis may also issue additional situation-based products on emerging threats. The Pipeline Modal and Cyber Modal Threat Assessments evaluate, respectively, physical and cyber threats to pipelines. The pipeline modal threat assessment evaluates terrorist threats to hazardous liquid and natural gas pipelines, and the cyber modal threat assessment evaluates cyber threats to transportation, including pipelines. Both assessments specifically analyze the primary threat actors, their capabilities, and activities—including attacks occurring internationally—as well as other characteristics of threat.

The Transportation Sector Security Risk Assessment assesses threat, vulnerability, and consequence for various attack scenarios across the five transportation modes for which TSA is responsible.⁷⁰ The scenarios define a type of threat actor—including homegrown violent extremists and transnational extremists, such as al Qaeda and its affiliates—a target, and an attack mode. For example, a scenario might assess the risk of attacks using varying sizes of improvised explosive devices on pipeline system assets. As part of the assessment process, TSA engages with subject matter experts from TSA and industry stakeholder representatives to compile vulnerabilities for each mode, and TSA analyzes both direct and indirect consequences of the various attack scenarios. According to Pipeline Security Branch of-

⁶⁹ GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 10, 2014).

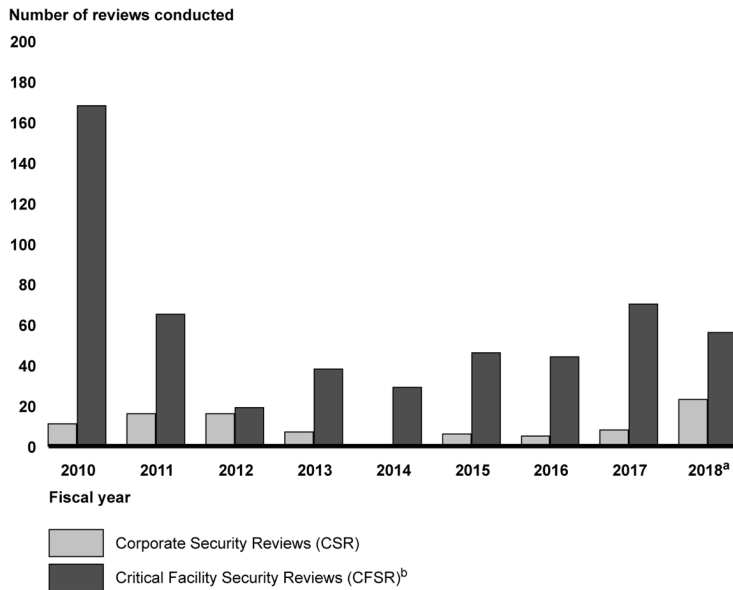
⁷⁰ According to TSA, the Transportation Sector Security Risk Assessment was developed both in response to requirements in statute to conduct risk assessments for the Transportation Systems sector and to fulfill TSA's operational and strategic need for a comprehensive risk assessment to aid in planning, risk-based decision making, and resource allocation. See, e.g., Pub. L. No. 110-53, § 1511, 121 Stat. 426-29 (2007); 6 U.S.C. § 1161 (requiring the submission of a nationwide risk assessment of a terrorist attack on railroad carriers). The five transportation modes for which TSA is responsible are: Aviation; Freight Rail; Highway; Pipeline; and Mass Transit.

ficials, the assessments produced by TSA's Intelligence and Analysis provide key information to inform the pipeline security program's efforts.

TSA Conducts Pipeline Security Reviews to Assess Implementation of Pipeline Guidelines, but Does Not Have a Strategic Workforce Plan to Address Staffing Challenges

According to TSA officials, TSA conducts pipeline security reviews—Corporate Security Reviews (CSRs) and Critical Facility Security Reviews (CFSRs)—to assess pipeline vulnerabilities and industry implementation of TSA's *Pipeline Security Guidelines*. However, as shown by Figure 7 below, the number of CSRs and CFSRs completed by TSA has varied during the last five Fiscal Years, ranging from zero CSRs conducted in Fiscal Year 2014 to 23 CSRs conducted in Fiscal Year 2018, as of July 31, 2018.⁷¹

Figure 7: Pipeline Security Reviews Conducted, Fiscal Year 2010 through July 2018



Source: GAO analysis of Transportation Security Administration-reported figures. | GAO-19-48

^a Fiscal year (FY) 2018 data are through July 31, 2018.

^b Fiscal years 2010 and 2011 represent Critical Facility Inspections, which were the predecessor to CFSRs.

TSA officials reported that staffing limitations have prevented TSA from conducting more reviews. As shown in table 3, TSA Pipeline Security Branch staffing levels (excluding contractor support) have varied significantly over the past 9 years ranging from 14 full-time equivalents (FTEs) in Fiscal Years 2012 and 2013 to one FTE in Fiscal Year 2014. They stated that, while contractor support has assisted with conducting CFSRs, there were no contractor personnel providing CSR support from Fiscal Years 2010 through 2017, but that has now increased to two personnel in Fiscal Year 2018.⁷²

⁷¹ According to TSA officials, the decline in CSRs from 2013 to 2015 was caused by travel restrictions during sequestration, as well a reorganization which moved the assessment function.

⁷² In addition to TSA pipeline personnel, pipeline security reviews received support from contractors and other personnel within TSA's Surface Division. TSA awards for contract support amounted to \$2,443,634 on Critical Facility Inspections from Fiscal Years 2008 to 2011, \$3,978,151 on CFSRs from Fiscal Years 2012 to 2016, \$2,233,928 on CFSRs from Fiscal Years 2017 to 2021, and \$2,366,481 on CSRs from Fiscal Years 2017 to 2021.

Table 3: TSA Pipeline Security Branch Staffing Levels, Fiscal Years 2010 through 2018

Fiscal Year	TSA Pipeline Security Branch Staffing ^a
2010	13
2011	13
2012	14
2013	14
2014	1
2015	6
2016	6
2017	6
2018	6

Source: Transportation Security Administration (TSA) documents. | GAO-19-48
^aTSA pipeline staffing numbers are in full-time equivalents.

TSA prioritizes reviewing and collecting information on the Nation's top 100 critical pipeline systems. According to TSA officials, they would need to conduct 46 CSRs in order to review the top 100 critical pipeline systems. In July 2018, TSA officials stated that TSA's current target was to assess each pipeline company every 2 to 3 years; this would equate to about 15 to 23 CSRs per year.⁷³ TSA officials stated that they expect to complete 20 CSRs and 60 CFSRs per Fiscal Year with Pipeline Security Branch employees and contract support, and have completed 23 CSRs through July 2018 for Fiscal Year 2018.

Given the ever-increasing cybersecurity risks to pipeline systems, ensuring that the Pipeline Security Branch has the required cybersecurity skills to effectively evaluate pipeline systems' cybersecurity is essential. Pipeline operators we interviewed emphasized the importance of cybersecurity skills among TSA staff. Specifically, 6 of the 10 pipeline operators and 3 of the 5 industry representatives we interviewed reported that the level of cybersecurity expertise among TSA staff and contractors may challenge the Pipeline Security Branch's ability to fully assess the cybersecurity portions of its security reviews. TSA officials stated that Security Policy and Industry Engagement staff are working with DHS's National Protection and Programs Directorate to help address cyber-related needs, including identifying specific cybersecurity skills and competencies required for the pipeline security program. The officials were uncertain, however, whether TSA would use contractor support or support from the National Protection and Programs Directorate to provide identified skills and competencies. TSA officials also stated that Security Policy and Industry Engagement staff work with TSA's human resource professionals to identify critical skills and competencies needed for Pipeline Security Branch personnel, and helps its workforce maintain professional expertise by providing training and education for any identified skill or competency gaps.

Our previous work has identified principles that a strategic workforce planning process should follow including developing strategies tailored to address gaps in number, deployment, and alignment of human capital approaches for enabling and sustaining the contributions of all critical skills and competencies.⁷⁴ Workforce planning efforts, linked to an agency's strategic goals and objectives, can enable it to remain aware of and be prepared for its needs, including the size of its workforce, its deployment across the organization, and the knowledge, skills, and abilities needed for it to pursue its mission. Agencies should consider how hiring, training, staff development, performance management, and other human capital strategies can be aligned to eliminate gaps and improve the long-term contribution of skills and competencies identified as important for mission success.⁷⁵

TSA has not established a workforce plan for its Security Policy and Industry Engagement or its Pipeline Security Branch that identifies staffing needs and skill sets such as the required level of cybersecurity expertise among TSA staff and contractors. When asked for TSA strategic workforce planning documents used to inform

⁷³To calculate the number of annual CSRs it would take to meet TSA's current target, we divided 46 CSRs by the number of years stated. For example, 46 CSRs divided by 2 years equals 23 CSRs per year; 46 CSRs divided by 3 years equals approximately 15 CSRs per year. This assumes that TSA does not review a pipeline company more than once in that time frame.

⁷⁴GAO, *Human Capital: Key Principles for Effective Strategic Workforce Planning*, GAO-04-39 (Washington, D.C.: Dec. 11, 2003).

⁷⁵GAO, *Human Capital: A Guide for Assessing Strategic Development Efforts in the Federal Government*, GAO-04-546G (Washington, D.C.: Mar. 1, 2004).

staffing allocations related to the pipeline security program, TSA officials acknowledged they do not have a strategic workforce plan. Rather, according to these officials, TSA determines agency-level staffing allocations through the Planning, Programming, Budgeting and Execution process, which is used to decide policy, strategy, and the development of personnel and capabilities to accomplish anticipated missions. According to TSA officials, when they use this process they look at existing resources and then set priorities based on the TSA Administrator's needs. However, a strategic workforce plan allows an agency to identify and prepare for its needs, such as the size of its workforce, its deployment across the organization, and the knowledge, skills, and abilities needed to pursue its mission. TSA officials stated that the agency has a detailed allocation plan for strategically aligning resources to screen passengers at TSA-regulated airports, but not for the entire agency.⁷⁶

By establishing a strategic workforce plan, TSA can help ensure it has identified the knowledge, skills, and abilities that the future workforce of TSA's Pipeline Security Branch may need in order to meet its mission of reducing pipeline systems' vulnerabilities to physical and cybersecurity risks, especially in a dynamic and evolving threat environment. Further, as greater emphasis is placed on cybersecurity, determining the long-term staffing needs of the Pipeline Security Branch will be essential. Furthermore, a workforce plan could enable TSA to determine the number of personnel it needs to meet its stated goals for conducting CSRs and CFSRs.

TSA Calculates Relative Risk of Pipeline Systems, but Its Ranking Tool Does Not Include Current Data or Align with DHS Priorities to Help Prioritize Security Reviews

After TSA identifies the top 100 critical pipeline systems based on throughput, the Pipeline Security Branch uses the Pipeline Relative Risk Ranking Tool (risk assessment), which it developed in 2007, to assess various security risks of those systems.⁷⁷ We previously reported, in 2010, that the Pipeline Security Branch was the first of TSA's surface transportation modes to develop a risk assessment model that combined all three components of risk—threat, vulnerability, and consequence—to generate a risk score.⁷⁸ The risk assessment generates a risk score for each of the 100 most critical pipeline systems and ranks them according to risk. The risk assessment calculates threat, vulnerability, and consequence for each pipeline system on variables such as the amount of throughput in the pipeline system and the number critical facilities. The risk assessment combines data collected from pipeline operators, as well as other Federal agencies, such as the Departments of Transportation and Defense, to generate the risk score.

However, the last time the Pipeline Security Branch calculated relative risk among the top 100 critical pipeline systems using the risk assessment was in 2014. Pipeline Security Branch officials told us that they use the pipeline risk assessment to rank relative risk of the top 100 critical pipeline systems, and the standard operating procedures for conducting CSRs state the results of the risk ranking are the primary factor considered when prioritizing corporate security reviews of pipeline companies.⁷⁹ According to Pipeline Security Branch officials, the risk assessment has not changed since 2014 because the Pipeline Security Branch is still conducting CSRs based on the 2014 ranking of pipeline systems.

As outlined in table 4 below, we identified several factors that likely limit the usefulness of the current risk assessment in calculating threat, vulnerability, and consequence to allow the Pipeline Security Branch to effectively prioritize reviews of pipeline systems. For example, because the risk assessment has not changed since

⁷⁶In 2018, we reported on TSA's airport staffing model and its use in assigning screening personnel to airports. See GAO, *Aviation Security: TSA Uses Current Assumptions and Airport-Specific Data for Its Staffing Process and Monitors Passenger Wait Times Using Daily Operations Data*, GAO-18-236 (Washington, D.C.: Feb. 1, 2018).

⁷⁷According to DHS, a risk assessment is a product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision-making. A risk assessment is also considered the appraisal of the risks facing an entity, asset, system, network, geographic area or other grouping. See DHS Risk Lexicon, 2010.

⁷⁸See GAO-10-867.

⁷⁹In August 2010, we recommended, among other things, that the Pipeline Security Branch document a methodology for scheduling CSRs that considers a pipeline system's risk ranking as the primary scheduling criteria and to balance that with other practical considerations. As a result, the Pipeline Security Branch revised its CSR Standard Operating Procedures, as documented in a copy dated May 20, 2011, to state that the primary criteria for scheduling CSR visits is the pipeline system's relative risk (*i.e.*, risk ranking), although other factors and considerations, such as operator availability and geographic location, will also play a role. Version 4.4, dated April 24, 2012, includes the same language. See GAO-10-867.

2014, information on threat may be outdated. Additionally, sources of data and underlying assumption and judgments regarding certain threat and vulnerability inputs to the assessment are not fully documented. For example, threats to cybersecurity are not specifically accounted for in the description of the risk assessment methodology, making it unclear if cybersecurity is part of the assessment's threat factor. Further, the risk assessment does not include information that is consistent with the NIPP and other DHS priorities for critical infrastructure risk mitigation, such as information on natural hazards and the ability to measure risk reduction (feedback data).

According to Pipeline Security Branch officials, the risk ranking assessment is not intended to be a fully developed risk model detailing all pipeline factors influencing risk. Rather, officials said they are primarily interested in assessing risk data that impacts security. However, because TSA's Pipeline Security Program is designed to enhance the security preparedness of the pipeline systems, incorporating additional factors that enhance security into their risk calculation would better align their efforts with PPD-21. For example, PPD-21 calls for agencies to integrate and analyze information to prioritize assets and manage risks to critical infrastructure, as well as anticipate interdependencies and cascading impacts. For a more detailed discussion of the shortfalls we identified, refer to appendix II.

Table 4: Shortfalls in the Pipeline Security Branch's Risk Ranking Assessment

Identified Shortfalls in the Risk Assessment	Shortfall Description and Corresponding Risk Element Affected: Threat (T), Vulnerability (V), Consequence (C)	Why It Matters
Information may be outdated	- The Pipeline Security Branch has not updated the risk assessment since June 2014, because of competing priorities. Therefore, information used to determine calculations, such as threat information, may be outdated and not reflect threats to the industry that have emerged in recent years. - When the risk assessment was last updated in 2014, it used pipeline systems' throughput data from 2010 to assess relative risk and throughput may have changed since 2010.	T - Standards for Internal Control in the Federal Government calls for management to use quality information to achieve the entity's objectives, including using relevant data from reliable sources obtained in a timely manner. - Keeping the risk assessment updated with current information could help the Pipeline Security Branch ensure it is using its limited resources to review the pipeline systems with greater risk. C
Data sources, underlying assumptions and judgments, and sources of uncertainty not always documented	- The Pipeline Security Branch ranked threat equally across pipeline systems because officials say they do not have enough threat information to distinguish threat by pipeline. However, this judgment is not documented in the risk assessment's methodology. - Threats to cybersecurity are not specifically accounted for in the description of the risk assessment methodology. - The number of critical facilities is part of a pipeline system's vulnerability score, but pipeline operators do not identify critical facilities consistently, leading to uncertainty in this input.	T - According to the National Infrastructure Protection Plan (NIPP), a risk assessment's methodology must clearly document what information is used and how it is synthesized to generate a risk estimate, including any assumptions, judgments, sources of uncertainty, and any implications for interpreting the results from the assessment. T V - Documenting sources of data and agency assumptions, judgments, or decisions to exclude information could provide increased transparency to those expected to interpret or use the results.
Does not include risk information consistent with the NIPP or other Department of Homeland Security (DHS) priorities for critical infrastructure risk mitigation, such as: data on prior attacks	The pipeline risk assessment includes a field that accounts for whether a pipeline experienced a previous security threat (including failed attacks). However, that field is not used in the risk assessment's calculation. Pipeline Security Branch officials acknowledged that prior attacks should be part of the threat calculation, but could not account for why they were not calculated for the systems in the risk assessment.	T - Information provided by the Pipeline Security Branch suggests some pipeline systems have experienced such threats. According to the NIPP, judgments, such as deciding not to include information, should be articulated in the methodology. - Including past attacks on pipeline systems could help the Pipeline Security Branch better differentiate threat among pipeline systems.

Table 4: Shortfalls in the Pipeline Security Branch's Risk Ranking Assessment—Continued

Identified Shortfalls in the Risk Assessment	Shortfall Description and Corresponding Risk Element Affected: Threat (T), Vulnerability (V), Consequence (C)	Why It Matters
natural hazards	The pipeline risk assessment does not account for natural hazards in its threat calculation. According to Pipeline Security Branch officials, there is not sufficient historical data available that would indicate a significant impact from natural disasters on pipeline infrastructure. However, we identified possible sources of data for the Pipeline Security Branch to consider, including information from the Federal Emergency Management Agency.	T - According to the NIPP, threat includes natural hazards with the potential to harm life, information, operations, the environment, and/or property. As such, natural disasters are a key element of the DHS's critical infrastructure security and resilience mission. - While there may not be historical data of natural hazard impact for every pipeline system, consulting other sources or experts could provide data or analysis for a more comprehensive threat picture.
feedback data on pipeline system performance, including cybersecurity	- The risk assessment is unable to measure the progress a pipeline system made in addressing vulnerability gaps between reviews, because Pipeline Security Branch officials said their current measure—a vulnerability score—is unreliable for comparative and analytic purposes. However, they agree on the importance of a feedback mechanism tying results of reviews to a revised vulnerability metric. - The risk assessment does not include a measure of cybersecurity vulnerabilities. According to Pipeline Security Branch officials, absent data specific to pipelines on their cyber vulnerabilities, they are unable to include a pipeline's vulnerability to cyber attack in the risk assessment.	V - The NIPP and DHS's Risk Management fundamentals emphasize the important role that a feedback mechanism plays in risk management. - As pipeline operators implement increasing levels of network technologies to control their systems, the Pipeline Security Branch may not be fully accounting for pipeline systems' cybersecurity activities by not including the cybersecurity-related vulnerabilities in its risk assessment inputs. Developing a feedback mechanism based on implementation of TSA's Pipeline Security Guidelines—including those on cybersecurity—could be an important input to the risk assessment's vulnerability calculation. This information would also inform the amount of risk pipeline companies are reducing by implementing the guidelines and could be used to inform overall risk reduction. V
physical pipeline condition	Pipeline physical condition is not accounted for in the current risk assessment. However, pipeline condition or location (such as above or below ground) could touch upon pipeline security as it relates to system vulnerability. According to the Transportation Systems Sector-Specific Plan, vulnerabilities to damage in aging transportation infrastructure—of which pipelines are a part—are projected to increase with continued climate change.	V - DHS has listed the potential for catastrophic losses to dramatically increase the overall risk associated with failing infrastructure and highlighted risks due to climate change and natural hazards to pipelines. The NIPP defines vulnerability as a physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given threat or hazard. - By considering additional information from DOT on the physical condition of a pipeline system, the Pipeline Security Branch could better inform its vulnerability calculations. Additionally, TSA could use the information to help pipeline operators identify security measures to help reduce vulnerability of an aging system because well-maintained, safe pipelines are more likely to tolerate a physical attack.
cross-sector interdependencies	The Pipeline Security Branch's pipeline risk assessment currently considers the effects of a pipeline system's ability to service assets such as major airports, the electric grid, and military bases. However, consequence is calculated on the loss or disruption of the pipeline system to these other assets and does not capture the dependency of the pipeline system on other energy sources, such as electricity. Pipeline Security Branch officials are considering cross-sector interdependencies and discuss these factors with operators as they relate to system resiliency, but did not see a direct link to pipeline security.	V - According to the NIPP, understanding and addressing risks from cross-sector dependencies and interdependencies is essential to enhancing critical infrastructure security and resilience. - Considering interdependencies of sectors in both directions could improve the calculations in the pipeline risk assessment.

Source: GAO Analysis of Transportation Security Administration Pipeline Relative Risk Ranking Tool data | GAO-19-48

TSA's Pipeline Risk Assessment Has Not Been Peer Reviewed to Help Validate the Data and Methodology

In addition to the shortfalls identified above, the risk assessment has not been peer reviewed since its conception in 2007. In our past work, we reported that independent, external peer reviews are a best practice in risk management and that

independent expert review panels can provide objective reviews of complex issues.⁸⁰ According to the National Research Council of the National Academies, external peer reviews should, among other things, address the structure of the assessment, the types and certainty of the data, and how the assessment is intended to be used. The National Research Council has also recommended that DHS improve its risk analyses for infrastructure protection by validating the assessments and submitting them to independent, external peer review.⁸¹

Other DHS components have implemented our prior recommendations to conduct peer reviews of their risk assessments.⁸² For example, in April 2013, we reported on DHS's management of its Chemical Facility Anti-Terrorism Standards (CFATS) program and found that the approach used to assess risk did not consider all of the elements of consequence, threat, and vulnerability associated with a terrorist attack involving certain chemicals.⁸³ The Infrastructure Security Compliance Division, which manages the CFATS program conducted a multiyear effort to improve their risk assessment methodology and included commissioning a peer review by the Homeland Security Studies and Analysis Institute, which resulted in multiple recommendations. As part of the implementation of some of the peer review's recommendations, DHS conducted peer reviews and technical reviews with government organizations and facility owners and operators, and worked with Sandia National Laboratories to verify and validate the CFATS program's revised risk assessment methodology, which was completed in January 2017.

According to Pipeline Security Branch officials, they are considering updates to the risk assessment methodology including changes to the vulnerability and consequence factors. These officials said the risk assessment was previously reviewed within the past 18 months by industry experts and they consider input from several Federal partners including DHS, DOT, and the Department of Defense. Officials also said they will consider input from industry experts and Federal partners while working on updating the risk assessment. However, most of the proposed changes to the risk assessment methodology officials described are ones that have been deliberated since our last review in 2010.⁸⁴ Therefore, an independent, external peer review would provide the opportunity for integration and analysis of additional outside expertise across the critical infrastructure community.

While independent, external peer reviews cannot ensure the success of a risk assessment approach, they can increase the probability of success by improving the technical quality of projects and the credibility of the decision-making process. According to the National Research Council of the National Academies, independent, external peer reviews should include validation and verification to ensure that the structure of the risk assessment is both accurate and reliable. Thus, an independent, external peer review would provide better assurance that the Pipeline Security Branch can rank relative risk among pipeline systems using the most comprehensive and accurate threat, vulnerability, and consequence information.

⁸⁰ See GAO, *Coast Guard: Security Risk Model Meets DHS Criteria, but More Training Could Enhance Its Use for Managing Programs and Operations*, GAO-12-14 (Washington, D.C.: Nov. 17, 2011); and *Aviation Security: Efforts to Validate TSA's Passenger Screening Behavior Detection Program Underway, but Opportunities Exist to Strengthen Validation and Address Operational Challenges*, GAO-10-763 (Washington, D.C.: May 20, 2011).

⁸¹ National Research Council of the National Academies, *Review of the Department of Homeland Security's Approach to Risk Analysis* (Washington, D.C., 2010).

⁸² See GAO, *Critical Infrastructure Protection: DHS Efforts to Assess Chemical Security Risk and Gather Feedback on Facility Outreach Can Be Strengthened*, GAO-13-353 (Washington, D.C.: Apr. 5, 2013). See also GAO, *Critical Infrastructure Protection: DHS List of Priority Assets Needs to Be Validated and Reported to Congress*, GAO-13-296 (Washington, D.C.: Mar. 25, 2013). In this March 2013 report, we found that changes to DHS's criteria for including assets on the National Critical Infrastructure Prioritization Program (NCIPP) list of the Nation's highest-priority critical infrastructure could hinder DHS's ability to compare infrastructure across sectors and that a peer review would better position DHS to reasonably assure that the NCIPP list identifies the Nation's highest priority critical infrastructure. DHS concurred with our recommendation, and in November 2013, DHS commissioned a seven-member panel to review the NCIPP process, which resulted in multiple observations, some of which DHS has taken steps to address. DHS's commissioning of a review panel satisfied the intent of our recommendation.

⁸³ See GAO-13-353.

⁸⁴ During our current review, Pipeline Security Branch officials reported that they are considering updates to the risk assessment methodology, including changes to vulnerability and consequence factors. However, the updates officials reported they were considering in 2018 are nearly identical to those that Pipeline Security Branch officials reported they were considering making in 2011 in response to our prior recommendation. These proposed changes were also present in the 2014 version of the risk assessment.

TSA Has Established Performance Measures, but Limitations Hinder TSA's Ability to Determine Pipeline Security Program Effectiveness

TSA has established performance measures, as well as databases to monitor pipeline security reviews and analyze their results. However, weaknesses in its performance measures and its efforts to record pipeline security review recommendations limit its ability to determine the extent that its pipeline security program has reduced pipeline sector risks. Furthermore, we identified data reliability issues in the information that TSA collects to track the status of pipeline security review recommendations, such as missing data, inconsistent data entry formats, and data entry errors.

TSA Has Established Performance Measures but Faces Challenges in Assessing the Effectiveness of Its Efforts to Reduce Pipeline Security Risks

TSA has three sets of performance measures for its pipeline efforts: the Pipeline Security Plan in the 2018 Biennial National Strategy for Transportation Security (NSTS), a management measure in the DHS Fiscal Year 2019 congressional budget justification, and summary figures in their CSR and CFSR databases. As a result of our 2010 work, TSA established performance measures and linked them to Pipeline Security Plan goals within the Surface Security Plan of the 2018 NSTS.⁸⁵ See table 5 below for the 2018 NSTS Pipeline Security Plan performance measures.

Table 5: 2018 NSTS Pipeline Security Plan Performance Measures, Goals 1 and 2

Goal	Objective	Outcome	Performance Measurement
NSTS Goal 1: Manage Risks to Transportation Systems from Terrorist Attack and Enhance System Resilience	Reduce the risks from a terrorist attack on pipeline systems through security plans addressing critical infrastructure protection, operational practices (to detect and deter), and cybersecurity.	Improvement of industry security plans and security planning through incorporation of TSA Pipeline Security Guidelines into existing security plans.	Percentage of critical pipeline systems implementing TSA Pipeline Security Guidelines as assessed through corporate and facility security reviews.
NSTS Goal 1: Manage Risks to Transportation Systems from Terrorist Attack and Enhance System Resilience	Conduct training of employees to identify, prevent, absorb, respond to, and recover from a terrorist attack.	Improved capability of the industry employees to identify, prevent, absorb, respond to, and recover from a physical and/or cyber terrorist attack.	Percentage of critical pipeline systems implementing TSA Pipeline Security Guidelines as assessed through corporate and facility security reviews.
NSTS Goal 1: Manage Risks to Transportation Systems from Terrorist Attack and Enhance System Resilience	Conduct exercises employing threat scenarios to evaluate and identify opportunities to improve security preparedness and resiliency.	Pipeline systems and public safety agencies are better prepared to respond and recover effectively in the event of security incidents.	Percentage of critical pipeline systems implementing TSA Pipeline Security Guidelines as assessed through corporate and facility security reviews.
NSTS Goal 2; Enhance Effective Domain Awareness of Transportation Systems and Threats	Maintain and enhance mechanisms for information and intelligence sharing between the pipeline industry and government.	Improved domain awareness through timely delivery of relevant intelligence and information products for pipeline industry to implement mitigation strategies to reduce risk.	Increased timely distribution of time sensitive intelligence products.
NSTS Goal 2; Enhance Effective Domain Awareness of Transportation Systems and Threats	Encourage industry engagement with first responders and the public to enhance understanding of community risks associated with pipeline systems.	Pipeline industry, first responders, and neighboring communities working collectively to plan and prepare for incidents that could disrupt pipeline operations and endanger the community.	Percentage of critical pipeline systems implementing TSA Pipeline Security Guidelines as assessed through corporate and facility security reviews.

Source: 2018 Biennial National Strategy for Transportation Security (NSTS) | GAO-19-48

⁸⁵ The NSTS provides biennial risk-based plans for transportation assets in the U.S. and identifies objectives which enhance the security of transportation infrastructure. The strategy includes a base plan, modal security plans, and an intermodal security plan. The Surface Security Plan includes four modal security plans: Mass Transit and Passenger Rail, Freight Rail, Highway and Motor Carrier, and Pipeline.

As shown in table 6 below, DHS also included a management measure in its Fiscal Year 2019 congressional budget justification to track the annual number of completed pipeline security reviews.

Table 6: Management Measure in DHS FY 2019 Congressional Budget Justification

Measure	Description
Number of High-Risk Pipeline Systems on Which Security Reviews Were Conducted.	Pipeline Security Reviews assess and elevate the security posture of the pipeline energy transportation mode. Information and recommendations from pipeline corporate headquarters and field site reviews inform critical energy facility operators of issues to enhance security from terrorism and criminal activity. The onsite security reviews develop firsthand knowledge of security planning and execution of the critical pipeline systems, establish communication with key pipeline security personnel, and identify and share smart practices. As industry wide security gaps are identified through the process, the TSA Surface Division develops programs to address gaps throughout the pipeline industry. Each pipeline corporation is assessed every 4 to 5 years.

Source: Department of Homeland Security (DHS) Transportation Security Administration (TSA) Fiscal Year (FY) 2019 Congressional Budget Justification | GAO-19-48

Finally, TSA Pipeline Security Branch officials said they use summary figures in the CFSR status database and the CSR goals and priorities database as performance measures.⁸⁶ For example, these include the percentage of CFSR recommendations implemented and the average percentage compliance with the guidelines by Fiscal Year.

We previously found that results-oriented organizations set performance goals to clearly define desired program outcomes and develop performance measures that are clearly linked to the performance goals.⁸⁷ Performance measures should focus on whether a program has achieved measurable standards toward achieving program goals, and allow agencies to monitor and report program accomplishments on an ongoing basis. Our previous work on performance metrics identified 10 attributes of effective performance.⁸⁸ Table 7 identifies each key attribute of effective performance measures along with its definition.

⁸⁶ TSA provided us with four databases containing CSR and CFSR information: Master CSR Recommendations Listing and Status (2010–2013), U-SSI CSR Data FY16–17 (10–10–2017), U-SSI—CFSR Recommendations (10–10–2017) Data (2010–2017), and U-SSI-CFSR Recommendations Analysis. The first contained information on CSR recommendations and their most recent status. The second contained information on CSRs conducted on pipeline operators and their compliance with the guidelines arranged by strategic goals and priorities. The third contained information on CFSR recommendations made by TSA. Finally, the fourth contained information on the most recent status of those CFSR recommendations. In order to better distinguish their contents, from here on we refer to them as the CSR recommendations database, the CSR goals and priorities database, the CFSR recommendations database, and the CFSR status database.

⁸⁷ GAO, *Executive Guide: Effectively Implementing the Government Performance and Results Act*, GAO/GGD-96-118 (Washington, D.C.: June 1996); *Managing for Results: Enhancing Agency Use of Performance Information for Management Decision Making*, GAO-05-927 (Washington, D.C.: Sept. 9, 2005); and *Veterans Justice Outreach Program: VA Could Improve Management by Establishing Performance Measures and Fully Assessing Risks*, GAO-16-393 (Washington, D.C.: Apr. 28, 2016).

⁸⁸ GAO, *Military Personnel: DOD Needs to Establish Performance Measures for the Armed Forces Sports Program*, GAO-17-542 (Washington, D.C.: June 8, 2017).

Table 7: Key Attributes of Effective Performance Measures

Attribute	Definition
Balance	A suite of measures ensures that an organization's various priorities are covered.
Clarity	Measure is clearly stated, and the name and definition are consistent with the methodology used to calculate it.
Core program activities	Measures cover the activities that an entity is expected to perform to support the intent of the program.
Government-wide priorities	Each measure covers a priority such as quality, timeliness, and cost of service.
Limited overlap	Measures provide new information beyond that provided by other measures.
Linkage	Measure is aligned with division-and agency-wide goals and mission and is clearly communicated throughout the organization.
Measurable target	Measure has a numerical goal.
Objectivity	Measure is reasonably free from significant bias or manipulation.
Reliability	Measure produces the same result under similar conditions.
Baseline and trend data	Measure has a baseline and trend data associated with it to identify, monitor, and report changes in performance and to help ensure that performance is viewed in context.

Source: GAO-17-542 | GAO-19-48

We evaluated the current performance measures included in the 2018 NSTS, the DHS Fiscal Year 2019 congressional budget justification, the CSR goals and priorities database, and the CFSR status database related to TSA's Pipeline Security Branch.

We primarily focused on key attributes which could be applied to individual measures. These include clarity, linkage, measurable targets, objectivity, reliability, and baseline and trend data. Our prior work on performance measurement found that all performance measure attributes are not equal and failure to have a particular attribute does not necessarily indicate that there is a weakness in that area or that the measure is not useful; rather, it may indicate an opportunity for further refinement.⁸⁹

Based on our evaluation, the TSA-identified measures do not possess attributes that we have identified as being key to successful performance measures. As a result, TSA cannot fully determine the extent to which the Pipeline Security Branch has achieved desired outcomes, including the effectiveness of its efforts to reduce risks to pipelines. Specifically, many of TSA's measures cover agency goals and mission, but they generally lack clarity and measurable targets, provide significantly overlapping information, and do not include baseline and trend data.

- **Clarity.** The pipeline-related measures in the 2018 NSTS are not clear because they do not describe the methodology used to calculate them, and the names and definitions are not clearly described. For example, NSTS goal 1 includes an objective to conduct training of employees responding to terrorist attacks. The desired outcome is to improve the capability of industry employees to respond and recover from terrorist attacks. However, the performance measure is the percentage of critical pipeline systems implementing the TSA *Pipeline Security Guidelines*. It is not clear if this measure is specific to the sections of the guidelines related to employee training or overall implementation of the guidelines. The CFSR status database measures include the percentage of recommendations implemented by topic, such as "Site Specific Security Measures," "Signage," or "Miscellaneous." However, the database does not specifically define these topics or explain the methodology for calculating the measures.⁹⁰ Unclear measures could be confusing and misleading to users.
- **Core program activities.** The pipeline-related measures in the 2018 NSTS cover some of the agency's core program activities, such as conducting security exercises with the pipeline industry and providing intelligence and information products to the industry. However, the NSTS Pipeline Security Plan measures do not specifically include some core program activities,⁹¹ such as updating the

⁸⁹ GAO, *Tax Administration: IRS Needs to Further Refine Its Tax Filing Season Performance Measures*, GAO-03-143 (Washington, D.C.: Nov. 22, 2002).

⁹⁰ Formula calculations provide some explanation of how the measures are calculated, although this may not be readily understood by users who are unfamiliar with spreadsheet formulas.

⁹¹ For the purposes of this report, the core program activities were those described in the *Pipeline Security Guidelines* and the 2018 NSTS Pipeline Security Plan. These include developing and updating the guidelines; conducting CSRs and CFSRs; conducting exercises to evaluate preparedness for, response to, and recovery from physical and cyber security incidents; providing

Continued

TSA *Pipeline Security Guidelines* or the results of conducting CSRs and CFSRs in order to collect the information necessary for the existing performance measures. The CSR goals and priorities database and the CFSR status database include measures intended to track some of the results of pipeline security reviews, such as the average percentage compliance with the guidelines by Fiscal Year and the percentage of CFSR recommendations implemented. If core program activities are not covered, there may not be enough information available in those areas to managers and stakeholders.

- *Limited overlap.* The pipeline-related measures in the 2018 NSTS do not have limited overlap. As discussed previously, four of the five NSTS measures are based on the percentage of critical pipeline systems implementing TSA's *Pipeline Security Guidelines*. The management measure is based on the number of complete pipeline security reviews. The CFSR status database measures are based on the percentage of recommendations implemented overall and by groups. Finally, the CSR goals and priorities database measures are based on the average compliance percentage of companies that had CSRs conducted in Fiscal Years 2016 and 2017. This is similar to four of the five NSTS measures. Significantly overlapping measures may lead to redundant, costly information that does not add value for TSA management.
- *Linkage.* The pipeline-related measures in the 2018 NSTS generally exhibited this key attribute. For example, all of the NSTS measures were arranged by agency strategic goals and risk-based priorities. However, the management measure in DHS's Fiscal Year 2019 congressional budget justification and the CFSR status database measures did not specify the TSA goals and priorities to which they were aligned. If measures are not aligned with division and agency-wide goals and mission, the behaviors and incentives created by these measures do not support achieving those goals or mission.
- *Measurable target.* TSA's measures generally did not include measurable targets in the form of a numerical goal and none of the NSTS measures had measurable targets. For example, the NSTS measure under the Security Planning priority, which tracks the percentage of critical pipeline systems implementing TSA's *Pipeline Security Guidelines*, does not state what specific percentages would be considered an improvement in industry security plans. However, the management measure did include target numbers of pipeline security reviews by Fiscal Year. Both the CFSR status database measures and CSR goals and priorities database measures did not include measurable targets. Without measurable targets, TSA cannot tell if performance is meeting expectations.
- *Objectivity.* Because the pipeline-related measures in the 2018 NSTS, the CFSR status database, and the CSR goals and priorities database generally lack clarity and measurable targets, TSA cannot ensure its measures are free from bias or manipulation, and therefore, are not objective. If measures are not objective, the results of performance assessments may be systematically overstated or understated.
- *Reliability.* Because the pipeline-related measures in the 2018 NSTS, the CFSR status database, and the CSR goals and priorities database generally lack clarity, measurable targets, and baseline and trend data, it is not clear if TSA's measures produce the same result under similar conditions; therefore, the pipeline-related measures are unreliable. If measures are not reliable, reported performance data may be inconsistent and add uncertainty.
- *Baseline and trend data.* TSA's measures generally did not include baseline and trend data. For example, none of the NSTS measures included past results and compared them to measurable targets. TSA officials were unable to identify measures or goals to assess the extent to which pipeline operators have fully implemented the guidelines or increased pipeline security, but did say developing a feedback mechanism to measure progress in closing vulnerability gaps was important. However, the management measure did include the number of completed pipeline security reviews for each Fiscal Year from 2014 through 2017, as well as numerical goals. The CFSR status database includes information on CFSRs conducted from May 22, 2012, through June 29, 2017, but the measures are calculated for the entire time period rather than year-by-year. The CSR goals and priorities database measures include percentage compliance with the guidelines for CSRs conducted in Fiscal Years 2016 and 2017, as well as a combined measure. However, baseline and trend data are not tracked or

timely and relevant intelligence and information to industry; and promoting pipeline security awareness in communities surrounding critical pipeline assets and systems.

reported in either database. Collecting, tracking, developing, and reporting baseline and trend data allows agencies to better evaluate progress being made and whether or not goals are being achieved.

Pipeline Security Branch officials explained that in addition to the measures reported in the 2018 NSTS Pipeline Security Plan, they primarily rely on measures assessing CSR and CFSR implementation for assessing the value of its pipeline security program. TSA officials reported that they collect and analyze data and information collected from CSRs and CFSRs to, among other things, determine strengths and weaknesses at critical pipeline facilities, areas to target for risk reduction strategies, and pipeline industry implementation of the voluntary *Pipeline Security Guidelines*. For example, TSA officials reported that they analyzed information from approximately 734 CFSR recommendations that were made during Fiscal Years 2012 through 2016. They found that pipeline operators had made the strongest improvements in security training, public awareness outreach and law enforcement coordination, and site specific security measures. The most common areas in need of improvement were 24x7 monitoring, frequency of security vulnerability assessments, and proper signage.

However, as described above, we found those measures also did not comport with key attributes for successful measures and we report below on reliability concerns for underlying data supporting those measures. In addition, while the Pipeline Security Branch may not rely on the measures included in the 2018 NSTS Pipeline Security Plan and the Fiscal Year 2019 congressional budget justification, they are important for reporting the status of pipeline security efforts to TSA as a whole and to external stakeholders such as Congress.

Taking steps to ensure that the pipeline security program performance measures exhibit key attributes of successful performance measures could allow TSA to better assess the program's effectiveness at reducing pipeline physical and cybersecurity risks. This could include steps such as modifying its suite of measures so they are clear, have measurable targets, and add baseline and trend data. Further examples include the following:

- Adding measurable targets consisting of numerical goals could allow TSA to better determine if the pipeline security program is meeting expectations. For example, measurable targets could be added to TSA's existing measures by developing annual goals for the percentage of recommendations implemented to the CFSR status database and then reporting annual results.
- To make measures clearer, TSA could verify that each measure has a clearly stated name, definition, and methodology for how the measure is calculated. For example, the NSTS objective for security training mentioned above could have more specific language explaining how the measure is calculated and whether it applies to pipeline operators' implementation of the training-related portions of the *TSA Pipeline Security Guidelines* or overall implementation.
- Finally, adding baseline and trend data could allow TSA to identify, monitor, and report changes in performance and help ensure that performance is viewed in context. For example, the NSTS measures, CFSR status database measures, and CSR goals and priorities database measures could have annual results from prior years. This could help TSA and external stakeholders evaluate the effectiveness of the pipeline security program and whether it is making progress toward its goals.

TSA Does Not Track the Implementation Status of Past CSR Recommendations, and Supporting Data Are Not Sufficiently Reliable

According to TSA officials, the primary means for assessing the effectiveness of the agency's efforts to reduce pipeline security risks is through conducting pipeline security reviews—Corporate Security Reviews (CSRs) and Critical Facility Security Reviews (CFSRs). However, TSA has not tracked the status of CSR recommendations for over 5 years and related security review data are not sufficiently reliable.

When conducting CSRs and CFSRs, TSA staff makes recommendations to operators, if appropriate. For example, a CSR recommendation might include a suggestion to conduct annual security-related drills and exercises, and a CFSR recommendation might include a suggestion to install barbed wire on the main gate of a pipeline facility. In response to recommendations that we made in our 2010 report, TSA developed three databases to track CSR and CFSR recommendations and their imple-

mentation status by pipeline facility, system, operator, and product type.⁹² In addition, the agency recently developed a fourth database to collect and analyze information gathered from pipeline operators' responses to CSR questions. TSA officials reported that they use this database to assess the extent that TSA's pipeline security program has met NSTS goals and Pipeline Security Branch priorities. TSA officials stated that they use the CSR goals and priorities database for follow-up on recommendations, indications of improvement in pipeline security, and as an input into TSA performance goals and measures, including the performance measures for the 2018 NSTS Pipeline Security Plan.

We found several problems with the databases that indicate that the pipeline security program data are not sufficiently reliable and do not provide quality information that is current, complete, and accurate. First, the CSR recommendations database only included information for reviews conducted from November 2010 through February 2013. TSA officials stated that the agency stopped capturing CSR recommendations and status information in 2014. A TSA official stated that one factor was that the pipeline staffing level was one FTE in Fiscal Year 2014. However, the Pipeline Security Branch did not resume entering CSR recommendation-related information when staffing levels rose to 6 FTEs in the following year and beyond. As a result, TSA is missing over 5 years of data for the recommendations it made to pipeline operators when conducting CSRs.

The agency collected some information from CSRs conducted in Fiscal Years 2016 and 2017 in the separate CSR goals and priorities database. However, this database does not include all of the information that TSA collects when conducting CSRs. Specifically, the CSR goals and priorities database does not state which companies were reviewed, what specific recommendations were made, or the current status of those recommendations, and only records operators' responses to 79 of the 222 CSR questions.

Second, our review identified instances of missing data, inconsistent data entry formats, and data entry errors in the four databases. For example:

- The CSR recommendations database had missing data in all 13 of the included fields and a data entry error shifted 50 observations into the wrong fields, impacting both the Status Date and Completion Code fields.⁹³
- The CSR goals and priorities database had seven entries with inconsistent data formatting and five of those entries were not taken into account when calculating summary figures.⁹⁴
- The CFSR recommendations database had missing data in 3 of 9 fields.⁹⁵ There was also inconsistent data entry formats in 3 fields.⁹⁶
- The CFSR status database had missing data in 7 of 29 fields⁹⁷ and inconsistent data entry formats in 4 fields.⁹⁸

Finally, TSA has not documented its data entry and verification procedures, such as in a data dictionary or user manual, and does not have electronic safeguards for out-of-range or inconsistent entries for any of the databases it uses to track the status of CSR or CFSR recommendations and analyze operator responses to the CSR. TSA Pipeline Security Branch officials told us that they had not documented data entry and verification procedures and did not have electronic safeguards. This was for two reasons. First, the officials stated that the databases are small and maintained in a commercial spreadsheet program that does not allow for electronic safe-

⁹² GAO, *Pipeline Security: TSA Has Taken Actions to Help Strengthen Security, but Could Improve Priority-Setting and Assessment Processes*, GAO-10-867 (Washington, D.C.: Aug. 4, 2010).

⁹³ For example, 3 fields had 1 percent or less missing data, 7 fields had approximately 2 percent, 2 fields had 17 percent, and 1 field had 18 percent. Further, we found that 6 out of 13 fields had inconsistent data entry formats or allowed unrestricted text entries. For example, the Status field describes the current status of TSA's recommendations and includes entries such as "1," "(1) Completed", and "Completed using alternative strategy".

⁹⁴ For example, in Fiscal Year 2017 under a CSR question related to elements addressed in the corporate security plan, Company 7 had a "1" entered for "Yes" under "Other." The entry does not include an explanation, and it is not included in the summary calculation for the company.

⁹⁵ For example, the City, Recommendation, and Group fields had approximately 1 percent missing data.

⁹⁶ For example, based on a legend included in the database, the Group field assigns values of 1 through 13 which represent different areas of physical security. However, there are three out-of-range entries of "0".

⁹⁷ For example, 1 field had 1 percent missing data, 3 fields had 5 percent, 2 fields had 32 percent, and 1 field had 46 percent.

⁹⁸ For example, the Status Date field included entries such as "4/11/2014", "Estimated Completion 12/31/2017", and "Evergreen/Annually".

guards. However, based on our review of the databases, the spreadsheet program does allow for a variety of electronic safeguards. For example, entries can be restricted to only allow selections from a drop-down list or only allow dates to be entered. Second, only a small number of TSA employees enter information into these databases. TSA officials explained that typically one TSA employee is responsible for entering information from pipeline security reviews, and another individual, usually whoever conducted the review, is tasked to verify the accuracy of the data entered. As a result, according to the officials, any errors would be self-evident and caught during these TSA employees' reviews.

Our work has emphasized the importance of quality information for management to make informed decisions and evaluate agencies' performance in achieving key objectives and addressing risks. The *Standards for Internal Control in the Federal Government* states that management should use quality information to achieve agency objectives, where "quality" means, among other characteristics, current, complete, and accurate.⁹⁹ In addition, DHS's Information Quality Guidelines state that all DHS component agencies should treat information quality as integral to every step of the development of information, including creation, collection, maintenance, and dissemination. The guidelines also state that agencies should substantiate the quality of the information disseminated through documentation or other appropriate means.¹⁰⁰

Without current, complete, and accurate information, it is difficult for TSA to evaluate the performance of the pipeline security program. Until TSA monitors and records the status of these reviews' recommendations, it will be hindered in its efforts to determine whether its recommendations are leading to significant reduction in risk. By entering information on CSR recommendations and monitoring and recording their status, developing written documentation of its data entry and verification procedures and electronic safeguards, and improving the quality of its pipeline security program data, TSA could better ensure it has the information necessary to effectively monitor pipeline operators' progress in improving their security posture, and evaluate its pipeline security program's effectiveness in reducing security risks to pipelines.

Conclusions

A successful pipeline attack could have dire consequences on public health and safety, as well as the U.S. economy. Recent coordinated campaigns by environmental activists to disrupt pipeline operations, and the successful attempts by nation-state actors to infiltrate and obtain sensitive information from pipeline operators' business and operating systems, demonstrate the dynamic and continuous threat to the security of our Nation's pipeline network.

To help ensure the safety of our pipelines throughout the nation, it is important for TSA to address weaknesses in the management of its pipeline security program. TSA's Pipeline Security Branch revised its security guidelines in March 2018 to, among other things, reflect the dynamic threat environment and incorporate NIST's Cybersecurity Framework cybersecurity principles and practices.¹⁰¹ However, without a documented process defining how frequently TSA is to review and, if deemed necessary, revise its guidelines, TSA cannot ensure that its guidelines reflect the latest known standards and best practices for physical and cybersecurity, or address the persistent and dynamic security threat environment currently facing the Nation's pipeline system. Further, without clearly defined criteria for determining pipeline facilities' criticality, TSA cannot ensure that pipeline operators are applying guidance uniformly and that all of the critical facilities across the pipeline sector have been identified; or that their vulnerabilities have been identified and addressed.

TSA could improve its ability to conduct pipeline security reviews and the means that it uses to prioritize which pipeline systems to review based on their relative risk ranking. Establishing a strategic workforce plan could help TSA ensure that it has identified the necessary skills, competencies, and staffing allocations that the Pipeline Security Branch needs to carry out its responsibilities, including conducting security reviews of critical pipeline companies and facilities, as well as their cybersecurity posture. Better considering threat, vulnerability, and consequence elements in its risk assessment and incorporating an independent, external peer re-

⁹⁹GAO-14-704G.

¹⁰⁰Department of Homeland Security, *Information Quality Guidelines*, (Washington, D.C.: Mar. 2011).

¹⁰¹Five of the 10 pipeline operators we interviewed characterized the guidelines as effective in helping to secure their operations, one operator was neutral, and the remaining four did not comment on the guidelines' effectiveness.

view in its process would provide more assurance that the Pipeline Security Branch ranks relative risk among pipeline systems using comprehensive and accurate data and methods.

TSA could also improve its ability to assess the extent to which the Pipeline Security Branch has met its goals. Taking steps to ensure that the pipeline security program performance measures exhibit key attributes of successful performance measures could allow TSA to better assess the program's effectiveness at reducing pipeline physical and cybersecurity risks. Without current, complete, and accurate information, it is difficult for TSA to evaluate the performance of the pipeline security program. By monitoring and recording the status of CSR recommendations, developing written documentation of its data entry and verification procedures and electronic safeguards, and improving the quality of its pipeline security program data, TSA could better ensure it has the information necessary to effectively monitor pipeline operators' progress in improving their security posture, and evaluate its pipeline security program's effectiveness in reducing security risks to pipelines.

Until TSA monitors and records the status of these reviews' recommendations, it will be hindered in its efforts to determine whether its recommendations are leading to significant reduction in risk.

Recommendations for Executive Action

We are making 10 recommendations to TSA:

- The TSA Administrator should direct the Security Policy and Industry Engagement's Surface Division to implement a documented process for reviewing, and if deemed necessary, for revising TSA's *Pipeline Security Guidelines* at regular defined intervals. (Recommendation 1)
- The TSA Administrator should direct the Security Policy and Industry Engagement's Surface Division to clarify TSA's *Pipeline Security Guidelines* by defining key terms within its criteria for determining critical facilities. (Recommendation 2)
- The TSA Administrator should develop a strategic workforce plan for its Security Policy and Industry Engagement's Surface Division, 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, that are needed to effectively conduct CSRs and CFSRs. (Recommendation 3)
- The TSA Administrator should direct the Security Policy and Industry Engagement's Surface Division to update the Pipeline Relative Risk Ranking Tool to include up-to-date data to ensure it reflects industry conditions, including throughput and threat data. (Recommendation 4)
- The TSA Administrator should direct the Security Policy and Industry Engagement's Surface Division to fully document the data sources, underlying assumptions and judgments that form the basis of the Pipeline Relative Risk Ranking Tool, including sources of uncertainty and any implications for interpreting the results from the assessment. (Recommendation 5)
- The TSA Administrator should direct the Security Policy and Industry Engagement's Surface Division to identify or develop other data sources relevant to threat, vulnerability, and consequence consistent with the NIPP and DHS critical infrastructure risk mitigation priorities and incorporate that data into the Pipeline Relative Risk Ranking Tool to assess relative risk of critical pipeline systems, which could include data on prior attacks, natural hazards, feedback data on pipeline system performance, physical pipeline condition, and cross-sector interdependencies. (Recommendation 6)
- The TSA Administrator should direct the Security Policy and Industry Engagement's Surface Division to take steps to coordinate an independent, external peer review of its Pipeline Relative Risk Ranking Tool, after the Pipeline Security Branch completes enhancements to its risk assessment approach. (Recommendation 7)
- The TSA Administrator should direct the Security Policy and Industry Engagement's Surface Division to ensure that it has a suite of performance measures which exhibit key attributes of successful performance measures, including measurable targets, clarity, and baseline and trend data. (Recommendation 8)
- The TSA Administrator should direct the Security Policy and Industry Engagement's Surface Division to take steps to enter information on CSR recommendations and monitor and record their status. (Recommendation 9)

- The TSA Administrator should direct the Security Policy and Industry Engagement's Surface Division to improve the quality of its pipeline security program data by developing written documentation of its data entry and verification procedures, implementing standardized data entry formats, and correcting existing data entry errors. (Recommendation 10)

Agency Comments and Our Evaluation

We provided a draft of this report to DHS, DOE, DOT, and FERC. DHS provided written comments which are reproduced in appendix III. In its comments, DHS concurred with our recommendations and described actions planned to address them. DHS, DOE, DOT, FERC, also provided technical comments, which we incorporated as appropriate. We also provided draft excerpts of this product to the American Petroleum Institute (API), the Association of Oil Pipe Lines, the American Gas Association (AGA), the Interstate Natural Gas Association of America (INGAA), the American Public Gas Association, and the selected pipeline operators that we interviewed. For those who provided technical comments, we incorporated them as appropriate.

With regard to our first recommendation, that TSA implement a documented process for reviewing, and if deemed necessary, for revising its *Pipeline Security Guidelines* at regular defined intervals, DHS stated that TSA will implement a documented process for reviewing and revising its Pipeline Security Guidelines at regular defined intervals, as appropriate. DHS estimated that this effort would be completed by March 31, 2019. This action, if fully implemented, should address the intent of the recommendation.

With regard to our second recommendation, that TSA clarify its *Pipeline Security Guidelines* by defining key terms within its criteria for determining critical facilities, DHS stated that TSA will clarify its Pipeline Security Guidelines by defining key terms within its criteria for determining critical facilities. DHS estimated that this effort would be completed by May 31, 2019. This action, if fully implemented, should address the intent of the recommendation.

With regard to our third recommendation, that TSA develop a strategic workforce plan for its Security Policy and Industry Engagement's Surface Division, DHS stated that TSA will develop a strategic workforce plan for the division, which includes determining the number of personnel necessary to meet the goals set for the Pipeline Security Branch, as well as the knowledge, skills, and abilities, including cybersecurity, that are needed to effectively conduct CSRs and CFSRs. DHS estimated that this effort would be completed by June 30, 2019. This action, if fully implemented, should address the intent of the recommendation.

With regard to our fourth recommendation, that TSA update the Pipeline Relative Risk Ranking Tool to include up-to-date data in order to ensure it reflects industry conditions, including throughput and threat data, DHS stated that TSA will update the Pipeline Relative Risk Ranking Tool to include up-to-date data in order to ensure it reflects industry conditions, including throughput and threat data. DHS estimated that this effort would be completed by February 28, 2019. This action, if fully implemented, should address the intent of the recommendation.

With regard to our fifth recommendation, that TSA fully document the data sources, underlying assumptions, and judgements that form the basis of the Pipeline Relative Risk Ranking Tool, including sources of uncertainty and any implications for interpreting the results from the assessment, DHS stated that TSA will fully document the data sources, underlying assumptions, and judgements that form the basis of the Pipeline Relative Risk Ranking Tool. According to DHS, this will include sources of uncertainty and any implications for interpreting the results from the assessment. DHS estimated that this effort would be completed by February 28, 2019. This action, if fully implemented, should address the intent of the recommendation.

With regard to our sixth recommendation, that TSA identify or develop other data sources relevant to threat, vulnerability, and consequence consistent with the NIPP and DHS critical infrastructure risk mitigation priorities and incorporate that data into the Pipeline Relative Risk Ranking Tool to assess relative risk of critical pipeline systems, DHS stated that TSA will identify and/or develop other sources relevant to threat, vulnerability, and consequence consistent with the NIPP and DHS critical infrastructure risk mitigation priorities. DHS also stated that TSA will incorporate that data into the Pipeline Risk Ranking Tool to assess relative risk of critical pipeline systems, which could include data on prior attacks, natural hazards, feedback data on pipeline system performance, physical pipeline condition, and cross-sector interdependencies. DHS estimated that this effort would be completed by June 30, 2019. This action, if fully implemented, should address the intent of the recommendation.

With regard to our seventh recommendation, that TSA take steps to coordinate an independent, external peer review of its Pipeline Relative Risk Ranking Tool, after the Pipeline Security Branch completes enhancements to its risk assessment approach, DHS stated that, after completing enhancements to its risk assessment approach, TSA will take steps to coordinate an independent, external peer review of its Pipeline Relative Risk Ranking Tool. DHS estimated that this effort would be completed by November 30, 2019. This action, if fully implemented, should address the intent of the recommendation.

With regard to our eighth recommendation, that TSA ensure that the Security Policy and Industry Engagement's Surface Division has a suite of performance measures which exhibit key attributes of successful performance measures, including measurable targets, clarity, baseline, and trend data, DHS stated that TSA's Surface Division's Pipeline Section will develop both physical and cyber security performance measures, in consultation with pipeline stakeholders, to ensure that it has a suite of performance measures which exhibit key attributes of successful performance measures, including measurable targets, clarity, baseline, and trend data. DHS estimated that this effort would be completed by November 30, 2019. This action, if fully implemented, should address the intent of the recommendation.

With regard to our ninth recommendation, that TSA take steps to enter information on CSR recommendations and monitor and record their status, DHS stated that TSA will enter information on CSR recommendations and monitor and record their status. DHS estimated that this effort would be completed by October 31, 2019. This action, if fully implemented, should address the intent of the recommendation.

With regard to our tenth recommendation, that TSA take steps to improve the quality of its pipeline security program data by developing written documentation of its data entry and verification procedures, implementing standardized data entry formats, and correcting existing data entry errors, DHS stated that TSA will develop written documentation of its data entry and verification procedures, implementing standardized data entry formats, and correcting existing data entry errors. DHS estimated that this effort would be completed by July 31, 2019. This action, if fully implemented, should address the intent of the recommendation.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until one day from the report date. At that time, we will send copies to the appropriate congressional committees; the Secretaries of Energy, Homeland Security, and Transportation; the Executive Director of the Federal Energy Regulatory Committee; and other interested parties. In addition, the report is available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact Chris Currie at (404) 679-1875 or curriec@gao.gov, and Nick Marinos at (202) 512-9342 or marinosn@gao.gov. Key contributors to this report are listed in appendix IV.

CHRIS P. CURRIE,

Director,

Homeland Security and Justice Issues.

NICK MARINOS,

Director,

Cybersecurity and Data Protection Issues.

LIST OF REQUESTERS

The Honorable Ron Johnson
Chairman
The Honorable Claire McCaskill
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Maria Cantwell
Ranking Member
Committee on Energy and Natural Resources
United States Senate

The Honorable Michael McCaul
Chairman
Committee on Homeland Security
House of Representatives

The Honorable John Katko
Chairman
Subcommittee on Transportation and Protective Security
Committee on Homeland Security
House of Representatives

The Honorable Peter DeFazio
Ranking Member
Committee on Transportation and Infrastructure
House of Representatives

The Honorable Frank Pallone
Ranking Member
Committee on Energy and Commerce
House of Representatives

The Honorable Daniel Lipinski
Member of Congress
House of Representatives

APPENDIX I: FEDERAL AND INDUSTRY SECURITY GUIDELINES AND STANDARDS FOR THE PIPELINE SECTOR

This appendix lists security guidance and guidance-related tools that the pipeline operators and industry association officials we interviewed identified as adopted or available in order to secure their physical and cyber operations. This list should not be considered to include all physical and cybersecurity guidance that may be available or used by all pipeline operators nor do all operators use all guidance listed.

Table 8: Federal and Industry Guidelines and Regulations Identified as Applicable to Security by Selected Pipeline Operators

Document Title
American Gas Association (AGA), AGA and Interstate Natural Gas Association of America (INGAA), Security Practices Guidelines Natural Gas Industry Transmission and Distribution, May 2008
American National Standards Institute (ANSI)/International Society of Automation (ISA)-95.00.01–CDV3, Enterprise-Control System Integration Part 1: Models and Terminology (2008)
American Petroleum Institute (API), Security Guidelines for the Petroleum Industry, Third Edition, April 2005
API, Pipeline SCADA Security, API Standard 1164, Second Edition, October 2016
Canadian Standards Association (CSA) Z246.1–17: Security Management for Petroleum and Natural Gas Industry Systems, March 1, 2017
CARVER (criticality, accessibility, recuperability, vulnerability, effect, and recognizability) + Shock Vulnerability Assessment Tool
Center for Internet Security Critical Security Controls
Department of Energy (DOE) ONG Cybersecurity Capability Maturity Model (ONG C2M2) program
Department of Homeland Security (DHS), Cyber Security Evaluation Tool (CSET)
DHS Chemical Facility Antiterrorism Standards (CFATS)
Department of Transportation, Federal Pipeline Safety Regulations
DHS Infrastructure Survey Tool
INGAA, Control System Cyber Security Guidelines for the Natural Gas Pipeline Industry, January 31, 2011
International Organization for Standardization (ISO) and International Electrochemical Commission (IEC), 17799/27001/27002, Information technology—Security techniques—Code of Practice for Information Security Management
ISO/IEC 27001:2005: Information technology—Security Techniques—Information Security Management Systems—Requirements
ISO 31000—Risk Management
International Electrotechnical Commission 62443—Security for Industrial Automation and Control Systems
Maritime Transportation Security Act of 2002 (Public Law 107–295)
National Energy Board (NEB) Onshore Pipeline Regulations (OPR) SOR/99–294, June 19, 2016
National Institute of Standards and Technology (NIST), Special Publication (SP) 800–53: Security and Privacy Controls for Federal Information Systems and Organizations, April 2013
NIST, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, April 16, 2018
NIST, SP 800–82: Guide to Industrial Control Systems (ICS) Security Revision 2, May 2015
North American Electric Reliability Corporation, Critical Infrastructure Protection (CIP) standards

Source: GAO analysis of pipeline operator information. | GAO–19–48

APPENDIX II: DESCRIPTION OF AREAS FOR IMPROVEMENT IN THE PIPELINE SECURITY BRANCH'S PIPELINE RELATIVE RISK RANKING TOOL

The Transportation Security Administration's (TSA) Pipeline Security Branch developed the Pipeline Relative Risk Ranking Tool (risk assessment) in 2007.¹ The risk assessment calculates threat, vulnerability, and consequence on variables such as the amount of throughput in the pipeline system (consequence input). Pipeline Security Branch officials told us that they use the pipeline risk assessment to rank relative risk of the top 100 critical pipeline systems, and the standard operating procedures for conducting Corporate Security Reviews (CSR) state the results of the risk ranking are the primary factor considered when prioritizing CSRs of pipeline companies.²

¹According to DHS, a risk assessment is a product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making. A risk assessment is also considered the appraisal of the risks facing an entity, asset, system, network, geographic area or other grouping. See DHS Risk Lexicon, 2010.

²In August 2010, we recommended, among other things, that the Pipeline Security Branch document a methodology for scheduling CSRs that considers a pipeline system's risk ranking as the primary scheduling criteria and to balance that with other practical considerations. As a result, the Pipeline Security Branch revised its CSR Standard Operating Procedures, as documented in a copy dated May 20, 2011, to state that the primary criteria for scheduling CSR

However, we identified several factors that likely limit the usefulness of the current assessment in calculating threat, vulnerability, and consequence to allow the Pipeline Security Branch to effectively prioritize reviews of pipeline systems. For example, because the risk assessment has not changed since 2014, information on threat may be outdated.

Additionally, sources of data and underlying assumption and judgments regarding certain threat and vulnerability inputs to the assessment are not fully documented. For example, threats to cybersecurity are not specifically accounted for in the description of the risk assessment methodology, making it unclear if cybersecurity is part of the assessment's threat factor. Further, the risk assessment does not include information that is consistent with the National Infrastructure Protection Plan (NIPP) and other Department of Homeland Security (DHS) priorities for critical infrastructure risk mitigation, such as information on natural hazards and the ability to measure risk reduction (feedback data).

According to Pipeline Security Branch officials, the risk ranking assessment is not intended to be a fully developed risk model detailing all pipeline factors influencing risk. Rather, officials said they are primarily interested in assessing risk data that impacts security. However, because TSA's Pipeline Security Program is designed to enhance the security preparedness of the pipeline systems, incorporating additional factors that enhance security into their risk calculation of the most critical pipeline systems would better align their efforts with Presidential Policy Directive 21 (PPD-21). For example, PPD-21 calls for agencies to integrate and analyze information to prioritize assets and manage risks to critical infrastructure, as well as anticipate interdependencies and cascading impacts.

Below we present the various shortfalls in the risk assessment—outdated data, limited description of sources and methodology, and opportunities to better align with the NIPP and other DHS priorities for critical infrastructure risk mitigation—in the context of the components that comprise a risk assessment: threat, vulnerability, and consequence.

Whereas in 2010 we made recommendations to improve the consequence component in the pipeline relative risk ranking tool, we have currently identified shortfalls that cut across all risk components: threat, vulnerability, and consequence.

Threat

We identified several shortfalls in the pipeline risk assessment's calculation of threat. First, while the risk assessment assesses consequence and vulnerability by pipeline system through use of multiple variables, it currently ranks threat for pipeline systems equally. Second, the evolving nature of threats to pipelines may not be reflected, since the risk assessment was last updated in 2014. Third, the threat calculation does not take into account natural hazards.

Pipeline Security Branch officials said they currently rank threat equally across pipeline systems because they do not have granular enough threat information to distinguish threat by pipeline. However, ranking threat equally effectively has no effect on the risk calculation for pipeline systems. Further, this judgment is not documented in the risk assessment's methodology. According to the NIPP, a risk assessment's methodology must clearly document what information is used and how it is synthesized to generate a risk estimate, including any assumptions and judgments. Additionally, our analysis of the pipeline risk assessment found that it includes at least one field that TSA could use to differentiate threat by pipeline. Specifically, the risk assessment includes a field that accounts for whether a pipeline experienced a previous security threat (including failed attacks), and information provided by Pipeline Security Branch suggests some pipeline systems have experienced such threats.

However, the Pipeline Security Branch did not capture these events in the risk assessment's calculation, which Pipeline Security Branch officials said should be part of the threat calculation, but could not account for why they were not calculated for the systems in the risk assessment. These officials also clarified that incidents such as suspicious photography or vandalism do not constitute an attack to be accounted for in the threat calculation. Documenting such assumptions, judgments, or decisions to exclude information could provide increased transparency to those expected to interpret or use the results.

Pipeline Security Branch officials also said that they ranked threat equally because TSA Intelligence and Analysis data show that threats to the oil and natural gas sector have been historically low, and Intelligence and Analysis does not conduct

visits is the pipeline system's relative risk (*i.e.*, risk ranking), although other factors and considerations, such as operator availability and geographic location, will also play a role. Version 4.4, dated April 24, 2012, includes the same language. See GAO-10-867.

specific threat analysis against individual pipeline systems. However, the Pipeline Security Branch has not updated the risk assessment since June 2014; therefore, the threat information it used to determine threat calculations—and decide to rank threat equally—may be outdated and not reflect the threats to the industry that have emerged in recent years. In fact, pipeline operators we interviewed indicated that the types of threats that concern pipeline operators have evolved. For example, 5 of the 10 operators we interviewed indicated that environmental activists were an increased threat to the pipeline industry because they use sabotage techniques, such as valve turning and cutting in service pipelines with blow torches, against pipelines. Additionally, 6 of 10 pipeline operators we interviewed said cyber attacks from nation-state actors were a primary threat to their industry. Further, when TSA issued its revised *Pipeline Security Guidelines* in March 2018, it stated that its revisions to the guidelines were made to reflect the ever-changing threat environment in both the physical and cybersecurity realms. However, threats to cybersecurity are not specifically accounted for in the description of the risk assessment methodology. Recent Pipeline Modal and Cyber Modal Threat Assessments include cyber threats to the pipeline industry, but the description of the pipeline risk assessment’s methodology does not specify what types of threat assessments (sources) are used to calculate its threat score. To better align with the guidance in the NIPP for documenting sources of information when conducting risk assessments, the Pipeline Security Branch should document the information used. Keeping the risk assessment updated with current information, as well as documenting those data sources, could help the Pipeline Security Branch ensure it is using its limited resources to review the pipeline systems with greater risk.

Natural Hazard Threats to Pipelines

The Transportation Systems Sector, of which pipelines are a part, is critical to the Pacific Northwest, but also at risk from natural hazards, like earthquakes. For example, according to the Department of Homeland Security, an earthquake in the Puget Sound region—which relies on the transportation of crude oil from Alaska—could cripple the ports of Seattle and Tacoma, as well as the Olympic and Williams Pipelines greatly impacting the Pacific Northwest Economic Region.

Hurricanes are the most frequent disruptive natural hazard for the oil and natural gas subsector and can cause the shutdown of facilities in an area, even when the facilities themselves are not directly affected by the storms. For example, according to the U.S. Energy Information Administration, the flow of petroleum into the New York area via pipeline from the Gulf Coast relies on the ability to move it through major terminals. In August 2017, Hurricane Harvey caused major disruptions to crude oil and petroleum product supply chains, including those to New York Harbor from Houston, Texas via the Colonial Pipeline. Due to the hurricane, decreased supplies of petroleum products available for the pipeline in Houston forced Colonial Pipeline to limit operations temporarily.

Source: GAO analysis of agency information. | GAO-19-48

Vulnerability

Finally, another shortfall in the current pipeline risk assessment methodology is that it does not account for natural hazards in its threat calculation, even though DHS's definition of threat includes natural hazards, and security and resilience of critical infrastructure are often presented in the context of natural hazards.³ According to the NIPP, threat is a natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. As such, along with terrorism, criminal activity and cybersecurity, natural disasters are a key element of DHS's critical infrastructure security and resilience mission.

According to Pipeline Security Branch officials, there is not sufficient historical data available that would indicate a significant impact from natural disasters on specific pipeline systems. However, we identified possible sources of data for the Pipeline Security Branch to consider. For example, a 2016 RAND Corporation study examined national infrastructure systems' exposure to natural hazards, including pipelines.⁴ Additionally, the Federal Emergency Management Agency (FEMA) has collaborated with stakeholders to develop the National Risk Index to, among other things, establish a baseline of natural hazards risk for the United States. While there may not be historical data of natural hazard impact for every pipeline system, consulting other sources or experts could provide regional data or analysis to build a more comprehensive threat picture to help distinguish threats by pipeline system. According to the NIPP, hazard assessments should rely not only on historical information, but also future predictions about natural hazards to assess the likelihood or frequency of various hazards.

We also identified multiple shortfalls in the vulnerability factors used in the risk assessment methodology, such as the potential uncertainty of the number of critical facilities and incorporating a feedback mechanism to calculate overall risk reduction. Other considerations for vulnerability calculations include physical condition of the pipeline system, cybersecurity activities, and interdependencies among sectors.

The number of critical facilities a pipeline system has identified is used as an input for its vulnerability calculation in the Pipeline Security Branch's risk assessment methodology. As discussed earlier, we identified deficiencies in TSA's criteria for identifying critical facilities, and found that well-defined criteria and consistent application of the criteria for identifying critical facilities could improve the results of the Pipeline Security Branch's risk assessment. Nevertheless, communicating in the risk assessment the uncertainty that may be inherent in this self-reported information would better align the risk assessment with the NIPP.

³From the DHS Risk Lexicon, 2010 Edition, threat is a natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. Presidential Policy Directive/PPD-21, *Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 12, 2013) also presents the security and resilience of critical infrastructure in the context of natural hazards.

⁴Henry H. Willis *et al.*, *Current and Future Exposure of Infrastructure in the United States to Natural Hazards*. (Santa Monica, Calif.: RAND Corporation, 2016), https://www.rand.org/pubs/research_reports/RR1453.html.

Measuring Effectiveness in a Voluntary Environment

According to the National Infrastructure Protection Plan, the use of performance metrics is an important step in the critical infrastructure risk management process to enable assessment of improvements in critical infrastructure security and resilience. The metrics provide a basis for the critical infrastructure community to establish accountability, document actual performance, promote effective management, and provide a feedback mechanism to inform decision making.

By using metrics to evaluate the effectiveness of voluntary partnership efforts to achieve national and sector priorities, critical infrastructure partners can adjust and adapt their security and resilience approaches to account for progress achieved, as well as changes in the threat and other relevant environments. Metrics are used to focus attention on areas of security and resilience that warrant additional resources or other changes through an analysis of challenges and priorities at the national, sector, and owner/operator levels.

Metrics also serve as a feedback mechanism for other aspects of the critical infrastructure risk management approach.

Source: Department of Homeland Security. | GAO-19-48

Another shortfall in the risk assessment is its inability to reliably measure the progress a pipeline system made in addressing vulnerability gaps between security reviews. The current risk assessment includes a CSR score as part of its vulnerability calculation, which was developed in part in response to our 2010 recommendation to use more reliable data to measure a pipeline system's vulnerability gap. However, during our review, Pipeline Security Branch officials said they plan to remove pipeline companies' CSR scores from the risk assessment calculations, because they and industry partners do not have confidence that the score appropriately measures a pipeline system's vulnerability. For example, Pipeline Security Branch officials explained that pipeline companies consider security factors differently, which can lead to variation in implementing risk reduction activities and by extension lead to different CSR scores. However, removing the CSR score eliminates the only feedback mechanism in the risk assessment from a pipeline company's actual security review conducted by the Pipeline Security Branch. The NIPP and DHS's Risk Management fundamentals emphasize the important role that such feedback mechanisms play in risk management. Officials from the Pipeline Security Branch agree on the importance of a feedback mechanism tying results of reviews to a revised vulnerability metric, but said they need a better measure than the current CSR score which is unreliable for comparative and analytic purposes. Developing a feedback mechanism based on implementation of TSA's *Pipeline Security Guidelines* could be an important input to the risk assessment's vulnerability calculation. This information would also inform the amount of risk pipeline companies

are reducing by implementing the guidelines and could be used to inform overall risk reduction.

The physical and cyber environments in which the pipeline sector operates also present vulnerabilities not accounted for in the pipeline risk assessment. In recent years, DHS has listed the potential for catastrophic losses to dramatically increase the overall risk associated with failing infrastructure and highlighted risks due to climate change and natural hazards to pipelines.⁵ For example, DHS reported extreme temperatures—such as higher and lower temperatures over prolonged periods of time—increase vulnerability to the critical infrastructure by causing elements to break and cease to function. Pipelines that freeze and then rupture can affect the energy and transportation systems sectors. As noted above, according to the NIPP, a natural or man-made occurrence or action with the potential to harm life is considered a threat, whereas vulnerability is defined as a physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given threat or hazard. While pipeline physical condition is typically thought of in context of safety, pipeline condition or location (such as above or below ground) could touch upon pipeline security as it relates to system vulnerability. For example, a pipeline system or segment of a system with a compromised physical condition due to corrosion or age could affect the system's vulnerability to threats and affect its ability to recover from such threats by potentially increasing the time a system is offline.

According to the Transportation Systems Sector-Specific Plan, vulnerabilities to damage in aging transportation infrastructure—of which pipelines are a part—are projected to increase with the continued effects of climate change. Further, according to TSA's *Pipeline Security and Incident Recovery Protocol Plan*, pipeline integrity efforts—including the design, construction, operation, and maintenance of pipelines—are important to pipeline security because well-maintained, safe pipelines are more likely to tolerate a physical attack.⁶ The Pipeline Security Branch already collects information from the Pipeline and Hazardous Materials Safety Administration (PHMSA) for its risk assessment, specifically information on High Consequence Area and High Threat Urban Area mileage.⁷ By considering additional information PHMSA collects on pipeline integrity, the Pipeline Security Branch could also use the information to help pipeline operators identify security measures to help reduce the consequences related to the comparatively higher vulnerability of an aging or compromised system. This would align with the Pipeline Security Branch's efforts to improve security preparedness of pipeline systems and could better inform its vulnerability calculations for relative risk ranking of pipeline systems.

Capturing cybersecurity in the risk assessment is also an area for improvement. Pipeline Security Branch officials told us they consulted with the National Cybersecurity and Communications Integration Center to revise TSA's *Pipeline Security Guidelines* to align with the National Institute of Standards and Technology (NIST) Cybersecurity Framework and that absent data specific to pipelines on their cybersecurity vulnerabilities, they are unable to include a pipelines' vulnerability to cyber attack in the risk assessment. However, the Pipeline Security Branch recently updated the security review questions asked of pipeline operators during corporate and critical facility reviews based on the recently updated *Pipeline Security Guidelines*. Using these updated questions related to companies' cybersecurity posture, the Pipeline Security Branch could collect additional information on cybersecurity vulnerabilities which could inform the risk assessment. This could be an element of the feedback mechanism described above and emphasized in the NIPP. Additionally, NIST identified several supply chain vulnerabilities associated with cybersecurity, which are not currently accounted for in TSA's *Pipeline Security Guidelines*.⁸ As pipeline operators implement increasing levels of network tech-

⁵The Department of Homeland Security, *National Critical Infrastructure Protection and Resilience Annual Report 2011–2012*, Washington, D.C., Aug. 2013.

⁶Transportation Security Administration, *Pipeline Security and Incident Recovery Protocol Plan*, March 2010.

⁷PHMSA defines “high consequence areas” differently for gas and hazardous liquid. For gas, high consequence areas typically include highly populated or frequented areas, such as parks. See 49 C.F.R. § 192.903. For hazardous liquid, high consequence areas include highly populated areas, other populated areas, navigable waterways, and areas unusually sensitive to environmental damage. See 49 CFR § 195.450. TSA regulations pertaining to rail transportation security define High Threat Urban Area as “an area comprising one or more cities and surrounding areas including a 10-mile buffer zone.” See 49 C.F.R. § 1580.3.

⁸According to NIST's *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, NIST Special Publication 800–161 (April 2015), there are three principal vulnerabilities to identify: (1) Access paths within the supply chain that would allow malicious actors to gain information about the system and ultimately introduce components that

nologies to control their systems, the Pipeline Security Branch may not be fully accounting for pipeline systems' cybersecurity posture by not including the cybersecurity-related vulnerabilities in its risk assessment inputs.

Consequence

Finally, we identified shortfalls in cross-sector interdependencies, which could affect vulnerability calculations. According to the NIPP, understanding and addressing risks from cross-sector dependencies and interdependencies is essential to enhancing critical infrastructure security and resilience. The Pipeline Security Branch's pipeline risk assessment currently considers the effects of a pipeline system's ability to service assets such as major airports, the electric grid, and military bases.

However, consequence is calculated on the loss or disruption of the pipeline system to these other assets and does not capture the dependency of the pipeline system on other energy sources, such as electricity. Weather events such as Gulf of Mexico hurricanes and Superstorm Sandy highlighted the interdependencies between the pipeline and electrical sectors. Specifically, according to a 2015 DHS annual report on critical infrastructure, power failures during Superstorm Sandy in 2012 closed major pipelines for 4 days, reducing regional oil supplies by 35 to 40 percent. The report goes on to say that the interconnected nature of infrastructure systems can lead to cascading impacts and are increasing in frequency.⁹ Pipeline Security Branch officials are considering cross-sector interdependencies and said they discuss these factors with operators as they relate to system resiliency. Considering interdependencies of sectors in both directions—such as calculating the likelihood that an input like electricity could fail and cause disruptions to critical pipelines—could improve the calculations in the pipeline risk assessment.

As previously discussed, the Pipeline Security Branch last calculated relative risk among the top 100 pipeline systems in 2014. When doing so, it used pipeline systems' throughput data from 2010 to assess relative risk. According to Pipeline Security Branch officials, the amount of throughput in pipeline systems does not change substantially year to year. However, Standards for Internal Control in the Federal Government calls for management to use quality information to achieve the entity's objectives, including using relevant data from reliable sources obtained in a timely manner. The Pipeline Security Branch uses throughput data as a consequence factor in the risk assessment to determine a pipeline system's relative risk score.¹⁰ Throughput changes could affect relative risk ranking and the Pipeline Security Branch's ability to accurately prioritize reviews based on relative risk.

could cause the system to fail at some later time; (2) Access paths that would allow malicious actors to trigger a component malfunction or failure during system operations; and (3) Dependencies on supporting or associated components that might be more accessible or easier for malicious actors to subvert than components that directly perform critical functions.

⁹The DHS report highlighted this element of risk management stating while sectors understand the direct impacts (*i.e.*, loss of life and economic consequences) from damaged or failing infrastructure, the dependencies and interdependencies associated with related service disruptions are not as well known.

¹⁰A pipeline system with higher throughput would be considered to have a higher consequence score.

APPENDIX III: COMMENTS FROM THE DEPARTMENT OF HOMELAND SECURITY



November 29, 2018

Chris P. Currie
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Nick Marinos
Director, Cybersecurity & Data Protection Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-19-48, "CRITICAL
INFRASTRUCTURE PROTECTION: Actions Needed to Address Significant
Weaknesses in TSA's Pipeline Security Program Management"

Dear Messrs. Currie and Marinos:

Thank you for the opportunity to review and comment on the draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

The Department remains committed to working with our Federal and private sector partners in the security and resilience of our Nation's critical pipeline infrastructure. As noted in the National Infrastructure Protection Plan (NIPP 2013), "[v]oluntary collaboration between private sector owners and operators (including their partner associations, vendors, and others) and their government counterparts has been and will remain the primary mechanism for advancing collective action toward national critical infrastructure security and resilience."

DHS is extremely proud of the work the Transportation Security Administration (TSA) has done to foster collaboration with the pipeline industry and significantly improve physical security and cybersecurity. This has included the publication of security guidelines, extensive information sharing, and the conduct and analysis of individual security reviews. For example, TSA conducted 62 Critical Facility Security Reviews (CFSRs) and 23 Corporate Security Reviews (CSRs) during fiscal year (FY) 2018.

In March 2018, TSA published an update to the TSA "Pipeline Security Guidelines," which included considerable input and collaboration with Federal and industry partners, and a complete update to the recommended cybersecurity measures. GAO's draft report notes, "[a]ll operators that GAO interviewed stated that they had implemented TSA's Pipeline Security Guidelines," and many indicated "the Guidelines were effective in helping to secure their operations." This is consistent with TSA's observations and data collected during CSRs and CFSRs.

Additionally, we were pleased to note that GAO's report recognized pipeline operators are receiving security information from a variety of sources including TSA, the National Cyber Security and Communications Integration Center, Information Sharing and Analysis Centers, fusion centers, industry associations, and the pipeline Sector Coordinating Council.

DHS and TSA recognize the challenging and evolving nature of the threat, particularly with regard to cybersecurity. DHS recently inaugurated the National Risk Management Center and one of its first projects is to partner with TSA to conduct 10 in-depth cybersecurity reviews with pipeline companies during FY 2019. Ongoing CSRs and these assessments will provide valuable insights on the status of cybersecurity measures in the industry.

GAO's report also determined the pipeline sector to be "resilient and versatile," and that pipeline operators have been able to rapidly respond to the adverse consequences of an incident and quickly restore pipeline service. Likewise, the report noted pipeline infrastructure includes redundancies that make the national system resilient.

All Federal programs, regardless of size, have room for improvement, and we appreciate GAO's efforts to identify areas for improvement in the TSA Pipeline Security program. However, the use of "significant weaknesses" in the report title is an unfortunate mischaracterization that does not accurately convey the overall program effectiveness or account for the substantial work TSA has accomplished.

The draft report contained 10 recommendations, with which the Department concurs. Attached find our detailed response to each recommendation. Technical comments were previously provided under separate cover.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,



JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Attachment

**Attachment: Management Response to Recommendations
Contained in GAO-19-48**

GAO recommended that the Administrator of the Transportation Security Administration:

Recommendation 1: Direct the Security Policy and Industry Engagement's Surface Division to implement a documented process for reviewing, and if deemed necessary, for revising TSA's "Pipeline Security Guidelines" at regular defined intervals.

Response: Concur. TSA Surface Division, Pipeline Section personnel will implement a documented process for reviewing and personnel revising TSA's "Pipeline Security Guidelines" at regular defined intervals, as appropriate. Estimated Completion Date (ECD): March 31, 2019.

Recommendation 2: Direct the Security Policy and Industry Engagement's Surface Division to clarify its TSA's "Pipeline Security Guidelines" by defining key terms within its criteria for determining critical facilities.

Response: Concur. TSA Surface Division, Pipeline Section personnel will clarify TSA's "Pipeline Security Guidelines" by defining key terms within TSA criteria for determining critical facilities. ECD: May 31, 2019.

Recommendation 3: Develop a strategic workforce plan for its Security Policy and Industry Engagement's Surface Division, 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, that are needed to effectively conduct CSRs and CFSRs.

Response: Concur. TSA Surface Division personnel will develop a Strategic Workforce Plan for the Division, which includes determining the number of personnel necessary to meet the goals set for our Pipeline Security Branch, as well as the knowledge, skills, and abilities, including cybersecurity, that are needed to effectively conduct CSRs and CFSRs. ECD: June 30, 2019.

Recommendation 4: Direct the Security Policy and Industry Engagement's Surface Division to update the Pipeline Relative Risk Ranking Tool to include up-to-date data in order to ensure it reflects industry conditions, including throughput and threat data.

Response: Concur. TSA Surface Division, Pipeline Section personnel will update the Pipeline Relative Risk Ranking Tool to include up-to-date data in order to ensure it reflects industry conditions, including throughput and threat data. ECD: February 28, 2019.

Recommendation 5: Direct the Security Policy and Industry Engagement's Surface Division to fully document the data sources, underlying assumptions and judgements that form the basis of the Pipeline Relative Risk Ranking Tool, including sources of uncertainty and any implications for interpreting the results from the assessment.

Response: Concur. TSA Surface Division, Pipeline Section personnel will fully document the data sources, underlying assumptions, and judgements that form the basis of the Pipeline Relative Risk Ranking Tool, including sources of uncertainty and any implications for interpreting the results from the assessment. ECD: February 28, 2019.

Recommendation 6: Direct the Security Policy and Industry Engagement's Surface Division to identify or develop other data sources relevant to threat, vulnerability, and consequence consistent with the NIPP and DHS critical infrastructure risk mitigation priorities and incorporate that data into the Pipeline Relative Risk Ranking Tool to assess relative risk of critical pipeline systems, which could include data on prior attacks natural hazards, feedback data on pipeline system performance, physical pipeline condition, and cross-sector interdependencies.

Response: Concur. TSA Surface Division, Pipeline Section personnel will identify and/or develop other sources relevant to threat, vulnerability, and consequence consistent with the NIPP and DHS critical infrastructure risk mitigation priorities, and incorporate that data into the Pipeline Risk Ranking Tool to assess relative risk of critical pipeline systems, which could include data on prior attacks, natural hazards, feedback data on pipeline system performance, physical pipeline condition, and cross-sector interdependencies. ECD: June 30, 2019.

Recommendation 7: Direct the Security Policy and Industry Engagement's Surface Division to take steps to coordinate an independent, external peer review of its Pipeline Relative Risk Ranking Tool, after the Pipeline Security Branch completes enhancements to its risk assessment approach.

Response: Concur. TSA Surface Division personnel will take steps to coordinate an independent, external peer review of its Pipeline Relative Risk Ranking Tool, after the Pipeline Security Branch completes enhancements to its risk assessment approach. Given this is an unfunded requirement, the necessary work on the other recommendations made in the report, the identification of an independent, external peer organization, and the potential need to develop a services contract for this

review, completion of this recommendation may require up to a year. ECD: November 30, 2019.

Recommendation 8: Direct the Security Policy and Industry Engagement's Surface Division to ensure that it has a suite of performance measures which exhibit key attributes of successful performance measures, including measurable targets, clarity, baseline, and trend data.

Response: Concur. TSA Surface Division, Pipeline Section personnel will ensure there is a suite of performance measures which exhibit key attributes of successful performance measures, including measurable targets, clarity, baseline, and trend data. Given the challenge in developing both physical and cyber security performance measures in consultation with pipeline stakeholders, the development of these performance measures will take one year. ECD: November 30, 2019.

Recommendation 9: Direct the Security Policy and Industry Engagement's Surface Division to take steps to enter information on CSR recommendations and monitor and record their status.

Response: Concur. TSA Surface Division, Pipeline Section personnel will enter information on CSR recommendation and monitor and record TSA status. Since this is an unfunded requirement, the resourcing for this recommendation requires the completion and execution of the strategic workforce plan (Recommendation 3), which will not be completed until June 30, 2019. ECD: October 31, 2019.

Recommendation 10: Direct the Security Policy and Industry Engagement's Surface Division to take steps to improve the quality of its pipeline security program data by developing written documentation of its data entry and verification procedures, implementing standardized data entry formats, and correcting existing data entry errors.

Response: Concur. TSA Surface Division, Pipeline Section personnel will improve the quality of its pipeline security program data by developing written documentation of its data entry and verification procedures, implementing standardized data entry formats, and correcting existing data entry errors. ECD: July 31, 2019.

APPENDIX IV: GAO CONTACT AND STAFF ACKNOWLEDGMENTS

GAO Contact

Staff Acknowledgments

Chris P. Currie at (404) 679-1875 or curriec@gao.gov

Nick Marinos at (202) 512-9342 or marinosn@gao.gov.

In addition to the contacts named above, Ben Atwater, Assistant Director; Michael W. Gilmore, Assistant Director; and Michael C. Lenington, Analyst-in-Charge, managed this assignment. Chuck Bausell, David Blanding, Dominick Dale, Eric Hauswirth, Kenneth A. Johnson, Steve Komadina, Susanna Kuebler, Thomas Lombardi, David Plocher, and Janay Sam made significant contributions to this report.

The CHAIRMAN. Imagine what might result if an attack on Colonial Pipeline happened to an electric company. It wouldn't just be

some small drivers unable to fill up or forced to pay at the pump. A grid disruption could have massive impacts to our economy. Lives could also be on the line. It would take months for the U.S. to recover from such a hostile attack in the shutdown of our electricity grid.

Electric companies are now working overtime to protect their system, but the Federal Government should be part of the solution. We need to bring about critical infrastructure investments in technology that can help the electricity grid and companies secure their networks from these kinds of intrusions.

For example, helping utilities install fiber optic technologies to run their transmission lines, helping them to create closed communication networks, using directed fiber links for grid monitoring and control that will insulate the electric grid from these kind of cyber attacks should be a major priority for this Administration.

These investments could also serve as backbone for other important communications systems throughout our rural communities that aren't currently being served. It also can help ensure the challenges that we face in some of our urban areas.

So I appreciate the recent steps the Department of Homeland Security has taken to bolster pipeline cyber-security and the recent release of a second Security Directive.

While these Directives are an initial step in the right direction, many of them are needed to ensure the security of the Nation's pipeline. While TSA has taken steps to address the weakness in overseeing the pipeline security, as I mentioned, the GAO report shows incomplete information for security risk assessments, age protocols for responding to security incidents, and obviously many of the workforce issues that we have previously addressed in this committee.

At one point TSA only had six individuals working on Pipeline Security Group and that number has now grown to 34, but they're covering 2.7 miles of pipeline and we need to increase our accountability over this issue.

So I look forward to hearing what our witnesses have to say about this very important issue of how we grow our security in such a critical area of our Nation's economy.

I'll now turn to the Ranking Member, Senator Wicker.

**STATEMENT OF HON. ROGER WICKER,
U.S. SENATOR FROM MISSISSIPPI**

Senator WICKER. Thank you, Senator Cantwell.

On May 7th of this year, malicious attackers attacked Colonial Pipeline's network and infected its computer system. This was a major wake-up call for the United States and for us as policy-makers.

Colonial was temporarily forced to shut down its pipeline, disrupting energy supplies running from Houston, Texas, to the doorstep of New York City. As a result, we witnessed fuel and gasoline shortages across the Southeast and the Mid-Atlantic.

The effect of this dramatic attack highlighted the very present risks from cyber crime to our national security.

Today's hearing is an opportunity to discuss how to prepare our critical infrastructure systems against emerging cyber threats and

how we can apply lessons learned from the Colonial Pipeline incident.

Our nation has roughly three million miles of pipelines transporting essential energy products across the United States. Those energy products keep our businesses running, our lights on, and our homes warm in the winter.

It is essential that this critical infrastructure be protected against cyber attacks like the one on Colonial Pipeline in May.

Having fuel supplies cutoff for extended periods of time is devastating to Americans and to our economy. Senator Cantwell has not overstated the problem or the risk.

I'm glad Administrator Pekoske is here today to help us understand the Transportation Security Administration's leading role in overseeing our pipeline cybersecurity. I appreciate TSA's ongoing efforts to enhance Federal pipeline cybersecurity programs to address growing cyber-security risks.

This has long been a priority for me and this committee. Last Congress I worked with Senator Cantwell on legislation to grow our cybersecurity workforce so that American companies and government agencies have the talent to protect their systems from criminals.

As the Federal Government considers ways to improve the cybersecurity framework of the pipeline sector, it will be increasingly important for the public and private sectors to coordinate their efforts more closely.

The vast majority of the Nation's critical infrastructure is owned and operated by the private sector. Utilizing the expertise of operators and the relevant safety regulators will lead to a more successful implementation of Security Directives from TSA.

Because cyber crimes and the technologies used to conduct these attacks are continuing to evolve, we should avoid a one-size-fits-all approach and ensure that Federal policy provides flexibility of response and adequately accounts for changing risks.

We need to ensure pipelines continue to be a safe means of product transportation and can operate without disruption, which is a top priority for this committee. Strong public/private partnerships are critical in protecting the Nation against attacks from state actors, such as China and Russia.

Coordination between government and industry is needed to improve information-sharing about emerging cyber threats and best practices to address them. Industry should also build strong relationships with their regulators and law enforcement to increase that collaboration.

No company should stand alone in the face of threats from countries that want to do us harm. Just the other day the Biden Administration publicly condemned the People's Republic of China for its cybersecurity campaigns. I appreciate that statement, but more action is needed to push back on threats from China and hold Beijing accountable for its malicious behavior.

I want to thank all our witnesses for being here today and I look forward to your testimony and our give and take during question and answer.

Thank you, ma'am.

The CHAIRMAN. Thank you, Senator Wicker, for those comments.

I also wanted to enter into the record a couple of articles, one by David Sanger of the *New York Times*: Pipeline Attacks Yields Urgent Lessons About the White House Cybersecurity, just one paragraph there.

“The bad news is they say was that American adversaries, not only super powers but terrorists and cyber criminals, learned just how little it takes to incite chaos across a large part of the country, even if they don’t break into the core of the electricity grid.”

So I want to enter that and an article by United Divide: Colonial Pipeline Hack Highlights Grid’s Disruption Even with IT Focus, Cyber Attacks and Colonial Pipeline Cyber Attacks Highlights Need for More Serious Energy Policy.

So we’ll enter those into the record.

[The information referred to follows:]

New York Times | <https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html>

PIPELINE ATTACK YIELDS URGENT LESSONS ABOUT U.S. CYBERSECURITY

The hack underscored how vulnerable government and industry are to even basic assaults on computer networks.

By David E. Sanger and Nicole Perlroth

Published May 14, 2021 Updated June 8, 2021

For years, government officials and industry executives have run elaborate simulations of a targeted cyberattack on the power grid or gas pipelines in the United States, imagining how the country would respond.

But when the real, this-is-not-a-drill moment arrived, it didn’t look anything like the war games.

The attacker was not a terror group or a hostile state like Russia, China or Iran, as had been assumed in the simulations. It was a criminal extortion ring. The goal was not to disrupt the economy by taking a pipeline offline but to hold corporate data for ransom.

The most visible effects—long lines of nervous motorists at gas stations—stemmed not from a government response but from a decision by the victim, Colonial Pipeline, which controls nearly half the gasoline, jet fuel and diesel flowing along the East Coast, to turn off the spigot. It did so out of concern that the malware that had infected its back-office functions could make it difficult to bill for fuel delivered along the pipeline or even spread into the pipeline’s operating system.

What happened next was a vivid example of the difference between tabletop simulations and the cascade of consequences that can follow even a relatively unsophisticated attack. The aftereffects of the episode are still playing out, but some of the lessons are already clear, and demonstrate how far the government and private industry have to go in preventing and dealing with cyberattacks and in creating rapid backup systems for when critical infrastructure goes down.

In this case, the long-held belief that the pipeline’s operations were totally isolated from the data systems that were locked up by DarkSide, a ransomware gang believed to be operating out of Russia, turned out to be false. And the company’s decision to turn off the pipeline touched off a series of dominoes including panic buying at the pumps and a quiet fear inside the government that the damage could spread quickly.

A confidential assessment prepared by the Energy and Homeland Security Departments found that the country could only afford another three to five days with the Colonial pipeline shut down before buses and other mass transit would have to limit operations because of a lack of diesel fuel. Chemical factories and refinery operations would also shut down because there would be no way to distribute what they produced, the report said.

And while President Biden’s aides announced efforts to find alternative ways to haul gasoline and jet fuel up the East Coast, none were immediately in place. There was a shortage of truck drivers, and of tanker cars for trains.

“Every fragility was exposed,” Dmitri Alperovitch, a co-founder of CrowdStrike, a cybersecurity firm, and now chairman of the think tank Silverado Policy Accelerator. “We learned a lot about what could go wrong. Unfortunately, so did our adversaries.”

The list of lessons is long. Colonial, a private company, may have thought it had an impermeable wall of protections, but it was easily breached. Even after it paid the extortionists nearly \$5 million in digital currency to recover its data, the company found that the process of decrypting its data and turning the pipeline back on again was agonizingly slow, meaning it will still be days before the East Coast gets back to normal.

"This is not like flicking on a light switch," Mr. Biden said Thursday, noting that the 5,500-mile pipeline had never before been shut down.

For the administration, the event proved a perilous week in crisis management. Mr. Biden told aides, one recalled, that nothing could wreak political damage faster than television images of gas lines and rising prices, with the inevitable comparison to Jimmy Carter's worse moments as president.

Mr. Biden feared that, unless the pipeline resumed operations, panic receded and price gouging was nipped in the bud, the situation would feed concerns that the economic recovery is still fragile and that inflation is rising.

Beyond the flurry of actions to get oil moving on trucks, trains and ships, Mr. Biden published a long-gestating executive order that, for the first time, seeks to mandate changes in cybersecurity.

And he suggested that he was willing to take steps that the Obama administration hesitated to take during the 2016 election hacks—direct action to strike back at the attackers.

"We're also going to pursue a measure to disrupt their ability to operate," Mr. Biden said, a line that seemed to hint that United States Cyber Command, the military's cyberwarfare force, was being authorized to kick DarkSide off line, much as it did to another ransomware group in the fall ahead of the presidential election.

Hours later, the group's Internet sites went dark. By early Friday, DarkSide, and several other ransomware groups, including Babuk, which has hacked Washington D.C.'s police department, announced they were getting out of the game.

DarkSide alluded to disruptive action by an unspecified law enforcement agency, though it was not clear if that was the result of U.S. action or pressure from Russia ahead of Mr. Biden's expected summit with President Vladimir V. Putin. And going quiet might simply have reflected a decision by the ransomware gang to frustrate retaliation efforts by shutting down its operations, perhaps temporarily.

The Pentagon's Cyber Command referred questions to the National Security Council, which declined to comment.

The episode underscored the emergence of a new "blended threat," one that may come from cybercriminals, but is often tolerated, and sometimes encouraged, by a nation that sees the attacks as serving its interests. That is why Mr. Biden singled out Russia—not as the culprit, but as the Nation that harbors more ransomware groups than any other country.



President Biden made clear that he was willing to take action to disrupt or shut down the criminal network behind the extortion. T.J. Kirkpatrick for The New York Times

“We do not believe the Russian government was involved in this attack, but we do have strong reason to believe the criminals who did this attack are living in Russia,” Mr. Biden said. “We have been in direct communication with Moscow about the imperative for responsible countries to take action against these ransomware networks.”

With DarkSide’s systems down, it is unclear how Mr. Biden’s administration would retaliate further, beyond possible indictments and sanctions, which have not deterred Russian cybercriminals before. Striking back with a cyberattack also carries its own risks of escalation.

The administration also has to reckon with the fact that so much of America’s critical infrastructure is owned and operated by the private sector and remains ripe for attack.

“This attack has exposed just how poor our resilience is,” said Kiersten E. Todt, the managing director of the nonprofit Cyber Readiness Institute. “We are overthinking the threat, when we’re still not doing the bare basics to secure our critical infrastructure.”

The good news, some officials said, was that Americans got a wake-up call. Congress came face-to-face with the reality that the Federal government lacks the authority to require the companies that control more than 80 percent of the Nation’s critical infrastructure adopt minimal levels of cybersecurity.

The bad news, they said, was that American adversaries—not only superpowers but terrorists and cybercriminals—learned just how little it takes to incite chaos across a large part of the country, even if they do not break into the core of the electric grid, or the operational control systems that move gasoline, water and propane around the country.

Something as basic as a well-designed ransomware attack may easily do the trick, while offering plausible deniability to states like Russia, China and Iran that often tap outsiders for sensitive cyberoperations.

It remains a mystery how DarkSide first broke into Colonial’s business network. The privately held company has said virtually nothing about how the attack unfolded, at least in public. It waited four days before having any substantive discussions with the administration, an eternity during a cyberattack.

Cybersecurity experts also note that Colonial Pipeline would never have had to shut down its pipeline if it had more confidence in the separation between its business network and pipeline operations.

“There should absolutely be separation between data management and the actual operational technology,” Ms. Todt said. “Not doing the basics is frankly inexcusable for a company that carries 45 percent of gas to the East Coast.”

Other pipeline operators in the United States deploy advanced firewalls between their data and their operations that only allow data to flow one direction, out of the pipeline, and would prevent a ransomware attack from spreading in.

Colonial Pipeline has not said whether it deployed that level of security on its pipeline. Industry analysts say many critical infrastructure operators say installing such unidirectional gateways along a 5,500-mile pipeline can be complicated or prohibitively expensive. Others say the cost to deploy those safeguards are still cheaper than the losses from potential downtime.

Deterring ransomware criminals, which have been growing in number and brazenness over the past few years, will certainly be more difficult than deterring nations. But this week made the urgency clear.

“It’s all fun and games when we are stealing each other’s money,” said Sue Gordon, a former principal deputy director of national intelligence, and a longtime C.I.A. analyst with a specialty in cyberissues, said at a conference held by The Cipher Brief, an online intelligence newsletter. “When we are messing with a society’s ability to operate, we can’t tolerate it.”



Colonial Pipeline hack highlights grid disruption risks even with IT-focused cyberattack, analysts say

Hackers unleashed ransomware on the largest refined products pipeline on the East Coast, leading to a voluntary pipeline shutdown.

Published May 11, 2021



Robert Walton
Reporter

The cyberattack on Colonial Pipeline illustrates how difficult it will be for electric utilities to protect their grids from disruption, experts say, even when attacks are primarily targeting information technology (IT) systems.

The Colonial ransomware attack never migrated into the pipeline's operational technology (OT) environment, and the company says the shutdown was a proactive safety measure. That's good protocol, security experts say, though it simultaneously exposes a vulnerability:

"If you have an attack on the IT network, the OT network is going to go down," according to electric utility sector security consultant Tom Alrich.

An attack on one ...

Colonial transports gasoline, jet fuel and other refined products, but experts say a similar attack on a natural gas pipeline could

have impacted combined cycle generation facilities. Federal power regulators are now calling for new pipeline security requirements.

The Colonial attack did not directly affect the electric sector, but that is beside the point, security experts say. U.S. critical infrastructure is under attack, with Colonial now sitting alongside SolarWinds and the Oldsmar, Florida, water facility hack as examples of the country's lagging security.

"Every electric utility, pipeline operator, power plant, or anything else related to the energy sector should view this [as an] attack on themselves," said Jerry Ray, chief operations officer at cybersecurity company SecureAge. "There's nothing that Colonial did or didn't do with its cybersecurity defenses that would significantly differ from that of any other major company within the industry."

"You can't have a ransomware attack on your IT network and not have it affect the OT network unless it's like one machine," Alrich said. "In theory," Colonial could have shut down the IT network and left its OT operating, "but in practice that's a very bad idea," he said.

OT networks often need some information from the IT side, so there can be operational impacts [of an IT attack], Alrich said. While the risk of malware migrating from IT to OT may be minimal, if it were to happen, the effects could be devastating.

The Federal Bureau of Investigation has identified the hackers behind the Colonial attack as Darkside, a group of cybercriminals that supply ransomware to other hackers.

The group acknowledged the disruption in a statement, but it said its attack was financially motivated and not designed to halt the pipeline's operation.

"Our goal is to make money and not creating problems for society," Darkside said in a statement. "From today, we introduce moderation and check each company that our partners want to encrypt to avoid social consequences in the future."

Experts say the economics of ransomware — cheap to deploy, and potentially very lucrative — means the problem will grow.

"This is not the first ransomware cyberattack on an oil and gas utility — and it won't be the last — but it is the most serious. It is also potentially one of the most successful cyberattacks against US critical national infrastructure," David Bicknell, principal analyst at GlobalData's Thematic Research, said in a statement.

FERC head calls for new pipeline security requirements

The Colonial attack led the head of the Federal Energy Regulatory Commission to call for consideration of pipeline cybersecurity standards similar to the North American Electric Reliability Corp.'s Critical Infrastructure Protection standards.

"It is time to establish mandatory pipeline cybersecurity standards similar to those applicable to the electricity sector," FERC Chair Richard Glick said in a statement. Glick was joined by Commissioner Allison Clements in the call for stricter requirements.

"Simply encouraging pipelines to voluntarily adopt best practices is an inadequate response to the ever-increasing number and sophistication of malevolent cyber actors," the regulators said.

The Colonial attack has revealed a "gap" in critical infrastructure security, said Yury Dvorkin, assistant professor of electrical and computer engineering at the New York University Tandon School of Engineering.

"While cyber intrusions can be identified in a timely fashion, that is before these exploits are operationalized to damage infrastructure, there is still a gap in cyber defense capabilities that would avoid the need of shutting down the entire infrastructure," Dvorkin said in an email.

Energy systems need tools to analyze, localize and isolate cyber threats "before they propagate and affect large portions of the infrastructure, thus increasing the likelihood of complete shut downs," he said, pointing to artificial intelligence and machine learning as a possible solution.

The Edison Electric Institute, which represents investor-owned utilities, is keeping an eye on how the Colonial hack could impart lessons to the electric power sector.

"As this investigation unfolds, it will be important to understand how control systems were impacted — if at all — and what mitigation was effective," Scott Aaronson, EEI's vice president for security and preparedness, said in a statement.

Attack should be a 'wake-up call for the electric side'

The proactive shutdown of the Colonial pipeline is a feature, not a bug, experts say.

"Assuming they are able to isolate the attack and bring the control systems back online within a few days, this will be a shining example of a company's ability to respond to and mitigate an attack," Nick Cappi, cyber vice president of portfolio strategy and enablement at Hexagon, said in an email.

However, higher fuel prices, shortages and rationing could result if Colonial is not back online soon, Cappi said.

The company issued a statement saying it is working to return to service "in a phased approach" with "the goal of substantially restoring operational service by the end of the week."

Security firms recommend multifactor authentication, tested incident response plans and off-site system backups to avoid similar ransomware attacks in the future.

"I would hope that the gas pipeline hack is a wake-up call for the electric side of the power industry. Imagine a similar attack on the power grid in the dead of summer," Rick Tracy, chief security officer and product manager at cybersecurity firm Telos Corp., said in an email. "How many heat-related deaths might occur in the hottest parts of the country? Let's not wait to find out."

The CHAIRMAN. So welcome to our witnesses. We have the Honorable David Pekoske, Administrator of the TSA. Welcome. Thank you for being here.

The Honorable Polly Trottenberg, Deputy Secretary of Transportation. Thank you for being here.

And Ms. Leslie Gordon, Acting Director of Homeland Security, Justice, Government Accountability Office, in Washington, D.C.

So welcome to all the witnesses.

Mr. Pekoske, Administrator Pekoske, we'll start with you. Again look forward to your testimony.

**STATEMENT OF HON. DAVID P. PEKOSKE, ADMINISTRATOR,
TRANSPORTATION SECURITY ADMINISTRATION**

Mr. PEKOSKE. Thank you, Chair Cantwell, Ranking Member Wicker, appreciate the opportunity to appear before you this morning, and I'm honored to testify alongside two distinguished government leaders: Deputy Secretary Polly Trottenberg and Acting GAO Director Leslie Gordon.

As I begin my testimony, I want to highlight the hard work and professionalism of the TSA workforce who continue to safeguard our transportation system, both aviation and surface, during this pandemic, and are meeting the challenge of providing security each day as millions of passengers return to travel this summer.

I appreciate the Committee's focus and their long-time priority on surface transportation security. Since the enactment of the TSA Modernization Act of 2018, we have substantially increased the number of people directly supporting the surface transportation security mission.

At Headquarters, we have a new Office of Surface Operations that is led by a member of the Senior Executive Service. We have a specific Pipeline Security Staff that has increased over sixfold to 39 FTEs and approximately 20 cyber positions in this office.

In the field, we now have five regional security directors, each with a staff of five, who have mission solely focused on surface transportation security. Supporting the regional security directors are 200 surface transportation security inspectors at 47 locations across the country.

Additionally, this committee authorized the Surface Transportation Security Advisory Committee or STSAC that provides the same strong advocacy function that the Aviation Security Advisory Committee has provided the aviation sector. This new advisory committee is off to an impressive start and, in addition to the Surface System Owners and Operators who are members, the STSAC includes membership from all the DOT Surface Modal Administrations, to include the Pipeline and Hazardous Materials Safety Administration, the Department of Energy, and two DHS components, CISA and the Coast Guard.

The threats to pipelines have been increasing as evidenced by a Joint Cybersecurity Advisory issued just last week by CISA and the FBI. This advisory provides information on a spear phishing and intrusion campaign by state-sponsored Chinese actors in late 2011 and early 2012.

CISA and FBI assessed that this activity was ultimately intended to help China develop cyber attack capabilities against U.S.

pipelines, to physically damage pipelines or disrupt pipeline operations.

While the advisory is just being made public, indicators of compromise were provided in 2012 to the affected companies and the pipeline industry stakeholders.

Recognizing the risk to pipelines, the TSA issued Pipeline Security Guidelines in 2011. The latest version was published in March 2018 and updated in April of this year.

These guidelines were collaboratively developed with industry and government partners and they were operationalized through voluntary corporate security reviews, critical facility security reviews, and validated architecture design reviews. More than 80 percent of the most critical pipeline companies have completed at least one of these reviews.

However, based on additional more recent intelligence information and the ransomware attack on the Colonial Pipeline in May, TSA, in full coordination with our interagency partners, has issued two Security Directives to meet this immediate security threat, reduce the vulnerability of our pipeline system, and immediately protect transportation security.

The first Security Directive was issued on the 28th of May. The contents of this Security Directive are not sensitive security information. It required critical pipeline owners and operators who represent 85 percent of the energy product moved by pipelines to report significant cyber incidents to CISA, to designate a cybersecurity coordinator available 24/7, and to review current activities against our guidelines on cybersecurity. We have a hundred percent response from the affected pipeline companies.

The second Security Directive was issued last Monday for the same companies as the first and it became effective yesterday. The contents of this second Security Directive are sensitive security information.

We used NIST Special Publications and the NIST Cybersecurity Framework in developing our directive. These are proven and tested cybersecurity best practices. They require specific mitigation measures, a comprehensive cybersecurity contingency and response plan, and cybersecurity architecture design and reviews.

It provides for submission and the accelerated review of alternate procedures and this Directive was developed in coordination with our interagency partners and with input from the affected pipeline companies and associations in advance.

I appreciate the thorough reviews GAO has conducted on pipeline security. They've issued two reports, one in December 2018 and one in June 2019. We have closed 12 of the 15 recommendations that GAO made which we concurred with, three remain open. I expect all three will be complete as soon as possible and thank GAO for the review and advice.

In closing, we are dedicated to protecting our Nation's pipelines and cooperation and collaboration with our government and private sector partners.

Thank you for your strong support of TSA and for the opportunity to testify this morning. I look forward to your questions. Thank you.

[The prepared statement of Mr. Pekoske follows:]

PREPARED STATEMENT OF HON. DAVID P. PEKOSKE, ADMINISTRATOR,
TRANSPORTATION SECURITY ADMINISTRATION,
U.S. DEPARTMENT OF HOMELAND SECURITY

Good morning, Chair Cantwell, Ranking Member Wicker, and distinguished Members of the Committee. I appreciate the opportunity to appear before you today to discuss the Transportation Security Administration's (TSA) role in pipeline security.

The nation's pipeline systems illustrate how vital critical pipeline systems are to the economy, our national security, and the livelihood of our country. Safeguarding these systems is a critical undertaking and requires extensive collaboration with pipeline owners and operators. The United States has more than 2.8 million miles of natural gas and hazardous liquid pipelines owned and operated by over 3,000 private companies. In addition to the pipelines themselves, the systems include critical facilities such as compressor and pumping stations, metering and regulator stations, interconnects, main line valves, tank farms and terminals, and automated systems used to monitor and control these facilities. Pipelines are susceptible to physical attacks and other acts of tampering and sabotage. Cyber intrusions into pipeline computer networks have the potential to negatively impact our national security, economy, commerce, and well-being.

Pipeline Staffing, Resourcing, and Expanding Internal Capabilities

To support the surface transportation security mission, TSA has developed surface transportation policies and regulations; supports the grant process for surface transportation-related security enhancements; conducts inspections and assessments of surface transportation operators to identify risk and provide risk mitigation strategies; and provides workforce training and exercise support. In response to the *TSA Modernization Act*, in October 2019, TSA established the Surface Operations office, which reports to the Executive Assistant Administrator for Security Operations. This organization is led by an Assistant Administrator and Deputy Assistant Administrator, both members of the Senior Executive Service, at TSA Headquarters, and five Regional Security Directors in the field, all at the Senior Executive Service level. The Regional Security Directors and their supporting staff have direct operational oversight of approximately 200 Surface Transportation Security Inspectors deployed in 47 field offices across the country. Since the passage of the *TSA Modernization Act*, TSA has expanded our pipeline security staff from six to 39 Full Time Equivalents (FTEs) working in field operations, headquarters operations, and policy development. These resources, both in our headquarters and in the field have allowed us to substantially increase our surface transportation security capability.

Further, in Fiscal Year (FY) 2020, TSA established and trained a 20-member field-based Pipeline Security Assessment Team (PSAT), which is comprised of credentialed Transportation Security Inspectors (TSIs) located around the Nation in order to expand TSA's support and engagement capacity with pipeline owners and operators. For cybersecurity efforts, we now have eight members from the PSAT team and TSA headquarters who completed comprehensive cybersecurity training, provided by Idaho National Labs. This was done in partnership with the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), and we are receiving additional cybersecurity certification in support of TSA's pipeline security mission.

TSA continues to expand its cybersecurity staffing and resourcing capabilities through the establishment of a Cybersecurity Operations Support Branch embedded within Surface Operations. As part of the 39 FTE previously mentioned, staffing for this Cyber Branch will include an additional 10 specialized cybersecurity personnel, all of whom are expected to be onboard in the next 60 days. This increase is a direct result of the Cyber Workforce Initiative implemented by DHS this year that allows direct hiring for individuals with the appropriate cybersecurity expertise. In addition to these newly hired cybersecurity experts, TSA has positioned additional field-based TSIs to undergo cybersecurity training and are on a career path to become cyber assessors within the surface transportation environment. This newly established field-based team will create an additional capability for local level cybersecurity outreach and establish a model for future professional cybersecurity career progression within TSA.

We will continue to evaluate and support implementation of cybersecurity best practices across the transportation sector and collaborate with other government agencies on surface cyber programs and engagements.

The TSA Surface Policy Division within the Policy, Plans, and Engagement office, in Operations Support, is also increasing its cybersecurity efforts and will expand its workforce specializing in cybersecurity from six positions to a total of nine within

the next 60 days. This resource will focus on the development of cybersecurity-related policy and guidance for surface transportation security.

Stakeholder Partnership

In 2003, TSA began assessing the state of security in the pipeline industry through its Corporate Security Review (CSR) program. The goals of the program were to develop first-hand knowledge of the security measures in place at critical pipeline sites and establish working relationships with key pipeline security personnel including the industry-established Oil and Natural Gas Sector Coordinating Council (ONG SCC). The initial CSRs identified smart security practices and laid the groundwork for TSA's Pipeline Security Guidelines. The Pipeline Security Guidelines, required by the *Implementing Recommendations of the 9/11 Commission Act of 2007*, went into effect in 2011 and with a 2018 revision, are still in use today and updated as necessary.

These Pipeline Security Guidelines provide a security structure for pipeline owners and operators to use in developing their security plans and programs and contain recommended security measures for both physical and cyber security that serve as the de facto industry standard. The Pipeline Security Guidelines were updated and republished in March 2018 with a significant emphasis on cybersecurity measures that are aligned with the National Institute of Standards and Technology (NIST) Cyber Security Framework. The guideline's cybersecurity measures were developed in coordination with industry and with Industrial Control System (ICS) expertise from CISA. In April of this year, the criteria for identifying critical pipeline facilities in the guidelines were further updated.

Through our efforts to expand pipeline security, we have focused on enhancing the security preparedness of the Nation's hazardous liquid and natural gas pipeline system. TSA has established a range of productive public-private partnerships to protect the transport of hazardous liquids and natural gas. This partnership includes collaboration with our Federal partners, such as CISA, the Department of Transportation (DOT), the Department of Energy, and the Department of Justice. We are also partnering with the Federal Energy Regulatory Commission through the Energy Government Coordinating Council (EGCC). In addition, TSA is providing input and support to the activities and initiatives of the ONG SCC and the Pipeline Working Group (PWG), which also serves as the Pipeline Subsector Coordinating Council (PSCC) of the Transportation Systems Sector.

To support pipeline owners and operators in securing their systems, TSA develops and regularly distributes security training materials for industry employees and partners to increase domain awareness and ensure security expertise is widely shared. These include a security awareness training program highlighting signs of terrorism and each employee's role in reporting suspicious activity, an IED awareness video for employees, and an introduction to pipeline security for law enforcement officers. To address cyber threats, the training materials, available since 2017, contain a cybersecurity toolkit for small and midsize businesses, offering guidance on how to incorporate cyber risk into their transportation system. Also included is a pocket-sized guide for frontline employees that outlines the most common types of cybersecurity threats and explains how transportation systems can protect their data, computer systems, and personal information.

Exercises, Assessments, and Site Reviews

TSA works with industry partners to assess and mitigate vulnerabilities and improve security through collaborative efforts including intelligence briefings, exercises, assessments, and on-site reviews. Through the Intermodal Security Training and Exercise Program (I-STEP), TSA provides the pipeline community with exercises, training, and security planning tools to strengthen company security plans, policies, and procedures. To date, TSA has conducted 21 ISTEP tabletop exercises specific to pipelines, with pipeline companies participating in numerous other exercises more broadly focused on all modes of transportation. Working with pipeline operators' security personnel, TSA conducts Pipeline CSRs, which assess the degree to which the Pipeline Security Guidelines' physical and cybersecurity measures are integrated into the operator's corporate security plan.

TSA also conducts Critical Facility Security Reviews on critical pipeline facilities for the most critical pipeline owners and operators to collect site-specific information on facility security policies, procedures, and physical security measures.

TSA is a partner with CISA's National Risk Management Center in the Pipeline Cybersecurity Initiative (PCI). The initiative was launched in 2018 to assist pipeline owners and operators to prepare for and respond to significant cyber events. Through the PCI initiative CISA, TSA, and Idaho National Laboratory assess the cybersecurity posture and preparedness of pipeline companies, analyze assessment

findings to develop risk mitigation strategies and identify support and informational tools that companies may use to address identified risks.

To promote a secure and resilient cybersecurity posture, TSA works directly with CISA to collaborate with pipeline owners and operators to offer cybersecurity architecture design reviews to assess a pipeline operator's critical infrastructure including information technology (IT) and operational technology (OT) systems. This assessment is intended to determine if OT systems are designed, built, and operated in a reliable, secure, and resilient manner. This assessment goes beyond a questionnaire-type assessment and includes traffic analysis from selected critical network segments. Pipeline owners and operators have expressed appreciation for these reviews over the years, understanding the value of identifying vulnerabilities to help better secure their physical and cyber systems.

Cybersecurity

On behalf of DHS, the Co-Sector Risk Management Agency for the Transportation Systems Sector (TSS) along with DOT, TSA serves as the executive agent with the U.S. Coast Guard for TSS and is responsible for developing, deploying, and promoting TSS-focused cybersecurity initiatives, programs, assessment tools, strategies, and threat and intelligence information-sharing products. TSA is in close alignment with CISA and coordinates on both a tactical and strategic level to raise the cybersecurity baseline across the transportation sector. As noted earlier, TSA participates in the EGCC and regularly collaborates with the ONG SCC and the PWG/PSCC on programmatic issues affecting the cybersecurity of pipeline systems.

TSA also supports DHS's cybersecurity efforts in alignment with the NIST Cybersecurity Framework (Framework). The Framework is designed to provide a foundation for industry to better manage and reduce their cyber risk. TSA shares information and resources and develops products for stakeholders to support their adoption of the Framework. TSA works closely with the pipeline industry to identify and reduce cybersecurity vulnerabilities, including facilitating classified briefings to increase industry's awareness of cyber threats.

Colonial Pipeline Incident

On May 7, 2021, the Colonial Pipeline Company announced it halted its pipeline operations due to a ransomware attack. This incident temporarily disrupted critical supplies of gasoline and other refined petroleum products throughout the East Coast. This was not the first cyber intrusion in our Nation to have a direct impact and cybersecurity incidents affecting surface transportation systems continue to be a growing and evolving threat.

In response to this cyber intrusion, TSA exercised its *Aviation and Transportation Security Act of 2001* authorities to strengthen the cybersecurity and resilience of pipeline owners and operators by issuing two Security Directives. The first Security Directive issued by TSA following the Colonial Pipeline incident requires pipeline owners and operators of critical hazardous liquid and natural gas pipelines or a liquefied natural gas pipeline facility to designate a Cybersecurity Coordinator who is required to be available to TSA 24/7 to coordinate cybersecurity practices and address any incidents that arise. The Cybersecurity Coordinator is also required to report significant cybersecurity incidents to CISA and assess their current cybersecurity posture against a specific set of measures within the Pipeline Security Guidelines. As part of this assessment, the owners and operators must identify any gaps, develop a remediation plan if necessary, and report the results to TSA and CISA.

All information reported to CISA pursuant to the Security Directive is securely shared with TSA and other Federal agencies as appropriate. Similarly, all information provided to TSA is securely shared with CISA and other Federal agencies as appropriate. By requiring the reporting of significant cybersecurity incidents, the Federal government is better positioned to understand the constantly changing threat of cyber events and the current and evolving risks to pipelines. The designation of Cybersecurity Coordinators will give TSA a known and consistent point of contact with critical pipeline owners and operators, allowing TSA to rapidly share security information and intelligence. The assessments will assist owners and operators and TSA to better understand the current state of cybersecurity practices in individual companies and across the industry.

TSA is pleased to report that all of the designated owner/operators have complied with requirements in the first Security Directive, including conducting a self-assessment within 30 days, naming a Cybersecurity Coordinator, and informing TSA of the designated individual and alternate(s). This is a testament to the long-standing security partnership developed over the years between TSA and this critical sector and industry's commitment to fulfill their required security responsibilities and take

action on this evolving threat. TSA, in partnership with CISA, is in the process of analyzing all assessments to identify further mitigation efforts.

In response to the ongoing cybersecurity threat to pipeline systems, on July 19, 2021, TSA issued a second Security Directive that requires owners and operators of TSA-designated critical pipelines that transport hazardous liquids and natural gas to implement a number of urgently needed protections against cyber intrusions.

The second Security Directive was developed in close coordination with Federal partners, including subject matter experts from CISA. TSA consulted with industry on the Security Directive and took their comments into consideration, including updating the security directive to incorporate some of the feedback received. The second Security Directive requires owners and operators of TSA-designated critical pipelines 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.

Conclusion

The pipeline system is crucial to U.S. national security, transportation, and our energy supply. These pipelines provide connections to other critical infrastructure upon which we depend, such as power plants and the aviation gasoline fuel supply for airplanes. TSA is dedicated to protecting our Nation's pipeline networks against evolving threats and continues to work collaboratively with our government and private partners to expand the implementation of intelligence-driven, risk-based policies and programs. TSA is committed to ensuring appropriate security measures are in place to increase the physical and cyber security posture of the natural gas and hazardous pipeline industry sub-sector in alignment with the risks this system faces. Thank you for the opportunity to discuss TSA's efforts to strengthen pipeline security, and I look forward to your questions.

The CHAIRMAN. Thank you, Administrator.

Deputy Secretary Trottenberg, thank you so much for being here.

STATEMENT OF HON. POLLY TROTTEMBERG, DEPUTY SECRETARY, DEPARTMENT OF TRANSPORTATION

MS. TROTTEMBERG: Thanks, Chair Cantwell, Ranking Member Wicker, and Members of the Committee, for the opportunity to testify this morning and for your support of the Department of Transportation.

I'm honored to be here with my colleagues, Administrator Pekoske and Acting Director Gordon, to discuss the security of our Nation's pipeline system.

In recent years advances in hardware, software, and computational capabilities have brought safety and efficiency benefits to our pipeline system. However, as we're discussing today, these advances are also introducing new cybersecurity risks.

We're facing persistent and increasingly sophisticated cyber attacks with serious consequences for our economy and our communities. These risks require proactive, coordinated, and agile responses.

Today I'll speak about DOT's role in pipeline and transportation cybersecurity, our collaboration with the Department of Homeland Security, other agencies, and the private sector, and some lessons learned from our response to the Colonial Pipeline attack.

DOT has different levels of responsibility over cyber-security, depending on the mode of transportation, the level of public versus private ownership, and the authorities of our sister agencies. DOT's Pipeline and Hazardous Materials Safety Administration, PHMSA, oversees the safe operation of nearly three million miles of pipelines, 17,000 underground storage tanks, more than a 160 liquefied natural gas facilities, and 1.2 million daily shipments of hazardous

materials. PHMSA has over 550 employees and a budget of \$288 million.

With respect to cybersecurity, PHMSA's leveraging its authorities in three critical areas: pipeline control room regulations, the nerve centers of pipeline system operations, integrity management plan requirements, and emergency response plan regulations.

PHMSA coordinates closely with DHS in the regulation of pipelines, particularly through its relationship with TSA as delineated in our most recent Memorandum of Understanding which promotes cooperation, communications, and non-duplication of efforts.

More broadly, my written testimony details other offices across DOT that work together to coordinate and manage cybersecurity risks, including implementing President Biden's Executive Order on Improving the Nation's Cybersecurity, as well as our work with TSA, CISA, and private sector stakeholders.

When the Colonial Pipeline cyber attack occurred on May 7th, President Biden directed a whole of government response. Under the leadership of Secretary Buttigieg, PHMSA engaged around the clock, collaborating with the pipeline company and monitoring the safety of the pipeline.

PHMSA worked closely with Colonial to manually restart and operate the pipeline which was unprecedented in the modern era and to move nearly a million barrels of fuel within days.

DOT also acted quickly through FMCSA, MARAD, and other agency partners to facilitate the transport of fuel by trucks and ships to affected areas.

I'd like to take a moment to thank the DOT team for their hard work during the Colonial Pipeline cyber attack and for all they do to keep our transportation system safe and secure.

Traditionally PHMSA regulates safe pipeline operations and TSA regulates cybersecurity, but the Colonial Pipeline cyber attack illustrates how these two missions intertwine, requiring collective action from different government agencies and the private sector.

Therefore, PHMSA is revisiting the Scope of Integrity Management Plan and Emergency Response Plan requirements for pipeline operators to ensure they account for cyber-security attack contingency.

PHMSA also continues to work closely with DHS and Federal partners and shares information we receive through our inspections.

The Colonial Pipeline cyber attack taught us many lessons, particularly the need for trusted and timely information-sharing as well as public and private sector partnership. It also underscored that we need to keep learning and adapting quickly to meet the increasingly complex and sophisticated cybersecurity challenges.

At DOT, we look forward to working with this committee, our sister agencies, and White House partners, as well as private sector stakeholders, to strengthen and protect our Nation's infrastructure.

Thank you again for the opportunity to testify and I look forward to your questions.

[The prepared statement of Ms. Trottenberg follows:]

PREPARED STATEMENT OF HON. POLLY TROTTENBERG, DEPUTY SECRETARY,
U.S. DEPARTMENT OF TRANSPORTATION

Chair Cantwell, Ranking Member Wicker, and Members of the Committee, thank you for the opportunity to testify before you today, and for your support of the Department of Transportation (DOT). I am honored to be here with TSA Administrator Pekoske to discuss the security of our Nation's pipeline system.

The nexus between transportation infrastructure and national security centers on global competitiveness, climate change, and cybersecurity. As a nation, we need to take all three seriously. Today we will focus on the cybersecurity of a critical component of our national infrastructure: the pipelines that help to fuel and power our homes, our businesses, and our cars, trucks, and airplanes.

I. Cybersecurity Risks that Threaten Transportation Safety

In recent years, advances in hardware, software, and computational capabilities have brought significant safety and efficiency benefits to our pipeline system. However, these advances, along with the merging of digital and physical systems and the increased reliance on data, are introducing new cybersecurity risks to the integrity and availability of pipeline operations. We face persistent and increasingly sophisticated cyber attacks. And the Colonial Pipeline ransomware attack starkly demonstrated how serious the consequences could be for a key part of our national economy and all the Americans who rely on it. These risks require proactive, coordinated, and agile responses.

Today, I will speak with you about DOT's role in pipeline and transportation cybersecurity; our collaboration with the Department of Homeland Security's (DHS's) Transportation Security Administration (TSA) and Cybersecurity and Infrastructure Security Agency (CISA), Department of Energy, which was the designated lead for the Colonial response, other agencies, and the private sector; and the lessons learned from our response to the Colonial attack.

II. DOT's Role and Modal Authorities

Depending on the mode of transportation, the level of public versus private ownership, and the authorities of our interagency partners, the Department of Transportation has different levels of authorities and responsibilities over cybersecurity.

DOT's Pipeline and Hazardous Materials Safety Administration (or "PHMSA") oversees pipeline safety. PHMSA protects the American people and the environment with the safe operation of nearly 3 million miles of pipelines, 17,000 underground storage tanks, and more than 160 Liquefied Natural Gas facilities, as well as the safe packaging and 1.2 million daily shipments of hazardous materials. Pipelines, the vast majority of which fall under private ownership, are a critical component of our energy transportation infrastructure and quite literally power the U.S. economy.

PHMSA has over 550 employees and a budget of \$288M. With respect to cybersecurity, PHMSA is pursuing the means to leverage its authorities to inspect and enforce three critical components of pipeline operations:

- Pipeline control room regulations, which are the "nerve centers" of pipeline system operations;
- Integrity management plan requirements; and
- Emergency response plan regulations.

Through these authorities, PHMSA regulates—and will regulate—at the nexus between safe pipeline operations and cybersecurity. We coordinate closely with DHS in the regulation of pipelines, particularly through the relationship between the Transportation Security Administration and PHMSA. A Memorandum of Understanding recently updated as directed by Congress in the TSA Modernization Act of 2018 delineates the roles and responsibilities of PHMSA and TSA regarding the regulation of pipelines. The MOU promotes communications, efficiency, and a non-duplication of efforts between PHMSA and TSA.

More broadly, many offices across DOT work together to manage cybersecurity risks across our transportation system. Our Office of Intelligence, Security, and Emergency Response engages with the National Security Council and interagency partners on a natural gas pipelines Industrial Control Systems Cybersecurity Initiative and other work to tackle cyber threats from adversaries who seek to compromise critical systems that are essential to U.S. national and economic security.

Our Policy office coordinates cybersecurity policy implementation across our nine Operating Administrations. Our Research and Technology office and Volpe National Transportation Systems Center support our Operating Administrations to conduct

research on cybersecurity solutions and best practices as well as gaps that require new approaches.

Finally, the Department's Office of the Chief Information Officer (OCIO) manages internal cybersecurity initiatives and has led our agency's response to the Executive Order on Improving the Nation's Cybersecurity (EO 14028). In support of this Executive Order, the OCIO is recruiting for new cybersecurity talent, has begun deploying new capabilities, initiated a data sensitivity review, and has developed new proposals to encrypt and protect data. The OCIO is also collaborating with DOT Human Resources on management of DOT's cybersecurity workforce.

Through all these efforts, DOT continues work with our sister agencies, especially TSA and CISA, to invest in world class research and pursue initiatives to address cybersecurity threats, including risks to future transportation technologies and innovations.

III. DOT's Collaboration with Federal and Private Sector Partners

When it comes to pipeline cybersecurity, coordination, and collaboration among our Federal partners is critical. Although DOT and TSA are the co-sector risk management agencies for transportation safety and security—including pipelines, CISA is the lead on cybersecurity risk across critical infrastructure. CISA provides alerts, warnings, advisories, guidance, and resources to help critical infrastructure owners and operators bolster their cyber defenses.

DOT amplifies CISA's outreach by further distributing their vital messages to sector stakeholders. DOT and DHS also encourage the stakeholders to adopt the voluntary National Institute of Standards and Technology Cybersecurity Framework, created through collaboration between industry and government.

Protecting against malicious cyber actors requires the Federal Government to partner with the private sector, which owns, operates, and manufactures most of America's pipeline systems. The private sector has a responsibility to adapt to the continuously evolving cyber threat environment, to build and operate products securely, and protect the security of critical infrastructure in partnership with the Federal Government.

IV. Colonial Pipeline Successful Response and Lessons Learned

When the Colonial Pipeline cybersecurity hack occurred on May 7, 2021, President Biden immediately directed a whole of government approach to respond to the attack. Under the leadership of Secretary Buttigieg, DOT acted quickly to facilitate the transport of fuel to affected regions, and to help get the pipeline system back up and running.

PHMSA engaged around the clock, monitored the safety of the pipeline, and worked with the pipeline company to help ensure a safe restart. With our support, within days, the Pipeline was able to move nearly a million barrels of fuel on a manual basis.

Traditionally, PHMSA regulates safe pipeline operations, and TSA regulates cybersecurity. However, as we saw with the Colonial Pipeline, cybersecurity can and does affect safe and reliable operations. In the wake of this incident, PHMSA is revisiting the scope of integrity management plan and emergency response plan requirements—to ensure they account for cybersecurity attack contingencies.

PHMSA also continues to work closely with DHS and Federal partners, and shares information we receive through our inspection processes.

V. Conclusion

The Colonial Pipeline cybersecurity incident spotlighted the importance of trusted and timely information sharing as well as public and private sector partnership in transportation cybersecurity. It also underscored that we need to keep learning and adapting quickly to meet increasingly complex and sophisticated cybersecurity challenges. DOT will continue to work across the Federal Government and with the private sector to advance the cybersecurity of the pipelines that fuel and sustain our Nation.

Our transportation infrastructure has long been a bedrock of our national security and economic prosperity. At DOT, we look forward to working with this Committee and our agency and White House partners to strengthen and protect that infrastructure. Thank you again for the opportunity to testify, and I will be happy to answer your questions.

The CHAIRMAN. Thank you.
Ms. Gordon, welcome.

**STATEMENT OF LESLIE V. GORDON,
ACTING DIRECTOR, HOMELAND SECURITY AND JUSTICE,
GOVERNMENT ACCOUNTABILITY OFFICE**

Ms. GORDON. Good morning. Chair Cantwell, Ranking Member Wicker, Members of the Committee, I'm very pleased to be with you today and Administrator Pekoske, Deputy Secretary Trottenberg, I'm happy to be here to discuss GAO's work on pipeline security.

The May ransomware cyber attack against Colonial Pipeline's information technology network exemplifies the cybersecurity threats to critical infrastructure that we have reported on for many years.

In 2018 our high-risk series on cybersecurity identifies the urgent need to protect cyber-critical infrastructure as one of the four major cybersecurity challenges for the Federal Government and it remains an urgent need.

This morning I want to highlight a few of the steps that TSA is taking to address some of the Pipeline Security Program weaknesses that we and others have identified and note that ongoing attention will be important.

TSA addressed 12 of GAO's 15 recommendations from our work in 2018 and 2019. It clarified pipeline security guidelines, improved performance monitoring, assessed staffing needs, and updated guidance on Federal roles and responsibilities between the TSA and PHMSA.

One recent step TSA took was to develop a strategic workforce plan to assess its staffing needs. Both the number and requisite skills, including cybersecurity, needed to effectively meet Pipeline Security Program mission. As a part of its workforce assessment and plan, TSA reported needing a 41 percent increase in staffing to perform the current and projected pipeline security mission.

Also, subsequent to the Colonial Pipeline attack in May, TSA issued a Security Directive that required, among other things, critical pipeline owner-operators to assess whether their current operations are consistent with TSA's recommended cybersecurity asset measures in its pipeline security guidelines, identify any gaps and remediation measures needed, and report the results to TSA and others. Previously, pipeline owner-operators' application of the pipeline guidelines was voluntary.

In preparation for this hearing, we reviewed the security measures for pipeline cyber assets in the guidelines and found that they do not include several known mitigation strategies for current cyber threats, including ransomware attacks.

In June TSA officials told us they anticipate updating the guidelines over the next year.

Last week TSA issued another Security Directive that requires critical pipeline owner-operators to implement specific cybersecurity mitigation measures, develop a cybersecurity contingency response plan, and undergo an annual cybersecurity architecture design review, among other things.

This Security Directive is placing significant additional cybersecurity requirements on private sector-owned pipeline owner-operators and likely will generate additional information for TSA on cybersecurity needs and likely add to TSA's volume of work.

Both directives will be in effect for 1 year while pipeline cybersecurity risks will continue.

This concludes my statement. I'd be happy to respond to your questions.

[The prepared statement of Ms. Gordon follows:]

PREPARED STATEMENT OF LESLIE V. GORDON, ACTING DIRECTOR, HOMELAND SECURITY AND JUSTICE, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

CRITICAL INFRASTRUCTURE PROTECTION

TSA Is Taking Steps to Address Some Pipeline Security Program Weaknesses

Chair Cantwell, Ranking Member Wicker, and Members of the Committee:

Thank you for the opportunity to discuss our work on the Transportation Security Administration's (TSA) efforts to secure oil and gas pipelines from physical and cyber threats. Pipelines are one type of critical infrastructure, which includes assets and systems that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our country. More than 2.7 million miles of pipelines transport and distribute natural gas, oil, and other hazardous liquids throughout the United States. People and businesses depend on these products to operate vehicles and machinery, heat homes, generate electricity, and manufacture products. A minor pipeline system disruption could result in commodity price increases, while prolonged pipeline disruptions could lead to widespread energy shortages.¹

Cyberattacks are among the most recent threats to the Nation's pipeline systems. In May 2021, malicious actors used DarkSide ransomware to conduct a cyberattack against Colonial Pipeline's information technology network.² This cyberattack exemplifies the cybersecurity threats to critical infrastructure that we have reported on for many years.³ In 1997, we designated information security as a government-wide high-risk area and expanded it in 2003 to include protecting cyber critical infrastructure.⁴ In 2018, our High Risk Series on cybersecurity identified the urgent need to protect cyber critical infrastructure as one of the four major cybersecurity challenges for the Federal government.⁵

TSA, within the Department of Homeland Security (DHS), has primary oversight responsibility for the physical security and cybersecurity of transmission and distribution pipeline systems.⁶ TSA's Pipeline Security Branch manages its pipeline security program. The Pipeline Security Branch first issued voluntary Pipeline Security Guidelines in 2011 and released revised guidelines in March 2018 and April 2021.⁷

In my testimony today, I will discuss: (1) actions TSA has taken to address weaknesses we have previously identified in its pipeline security program; (2) cybersecurity-related weaknesses we have previously identified in the Nation's pipeline systems that TSA has not fully addressed; and (3) TSA's guidance to pipeline owner/operators.

¹Transportation Security Administration, Biennial National Strategy for Transportation Security: Report to Congress (Washington, D.C.: Apr. 4, 2018).

²Ransomware is malicious software used to deny access to systems or data until a ransom is paid.

³GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, GAO-21-119SP (Washington, D.C.: March 2, 2021) and *High Risk Series: An Overview*, GAO-HR-97-1 (Washington, D.C.: February 1997). GAO maintains a high-risk program to focus attention on government operations that it identifies as high risk due to their greater vulnerabilities to fraud, waste, abuse, and mismanagement or the need for transformation to address economy, efficiency, or effectiveness challenges.

⁴GAO, *High-Risk Series: An Update*, GAO-03-119 (Washington, D.C.: January 2003).

⁵GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Washington, D.C.: Sep 06, 2018). GAO, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, GAO-21-288 (Washington, D.C.: March 24, 2021).

⁶Transmission pipelines are used to transport crude oil and natural gas from their respective gathering systems to refining, processing, or storage facilities. Transmission pipelines also transport refined petroleum products and natural gas to customers, for use or for further distribution. With very few exceptions, transmission pipelines are dedicated to the transportation of crude oil, refined petroleum products, or natural gas.

⁷Transportation Security Administration. *Pipeline Security Guidelines, March 2018 (with Change 1 (April 2021))*.

My discussion of the actions TSA has taken to address weaknesses in its pipeline security program and the cybersecurity weaknesses that it has not fully addressed is based on two reports we issued in December 2018 and June 2019, selected updates we conducted in May 2021, and related information from our 2021 High Risk Series reports.⁸ For these prior reports, we reviewed and analyzed relevant documents from TSA and other Federal entities, evaluated TSA pipeline risk assessment efforts, and interviewed TSA officials, including officials within TSA's Pipeline Security Branch. We interviewed representatives from five major industry associations and security personnel from 10 pipeline owner/operators to collect a range of perspectives on topics relevant to pipeline security.⁹ While the information gathered during the operator interviews cannot be generalized to all pipeline owner/operators, it provides a range of perspectives on a variety of topics relevant to pipeline security. Additional details on the scope and methodology are available in our published reports.

To describe TSA's requirements and guidance to pipeline owner/operators, we also reviewed TSA's recent Pipeline Security Directives, its Pipeline Security Guidelines, and three security alerts.¹⁰ The advisories we reviewed contained information on current cyber threats including ransomware and known mitigation strategies.¹¹ The advisories direct critical infrastructure owner/operators to adopt specific mitigation strategies, such as: implementing multifactor authentication for remote access to networks; investigating unauthorized connections; and addressing known vulnerabilities by applying software patches or adopting other controls.

We conducted the work upon which this statement is based in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Cybersecurity Threats to Pipeline Systems

The interstate pipeline system runs through both remote and highly populated urban areas, and transports oil, natural gas, and other hazardous liquids. In addition to their vulnerability to physical attacks, pipelines are vulnerable to cyberattacks or intrusions due to their increased reliance on computerized systems and electronic data—particularly industrial control systems.¹² Industrial control systems are increasingly connected in modern energy systems, allowing cyberattacks that originate in business IT systems to migrate to industrial control systems.¹³

The *2021 Annual Threat Assessment of the U.S. Intelligence Community* and the *2020 Homeland Threat Assessment*, among others, note that certain nations and

⁸ GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management*, GAO-19-48 (Washington, D.C.: Dec. 18, 2018); GAO, *Critical Infrastructure Protection: Key Pipeline Security Documents Need to Reflect Current Operating Environment*, GAO-19-426 (Washington, D.C.: June 5, 2019); and GAO-21-288.

⁹ We selected the 10 pipeline owner/operators from TSA's list of the top 100 critical pipeline systems and chose them to ensure a mixture of the following characteristics: (a) type of pipeline commodity transported (*i.e.*, natural gas, oil, and hazardous liquids); (b) volume of product transported; and (c) whether or not the pipeline owner/operators' critical facilities had been the subject of a TSA security review. We considered the location of selected owner/operators' pipeline systems to ensure that a single state or region was not overrepresented in our sample. We also observed TSA's security reviews at three critical pipeline facilities from among the 10 selected pipeline systems.

¹⁰ National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA), NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems, Alert (AA20-205A), July 23, 2020. CISA and the Federal Bureau of Investigation (FBI), DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks, Alert (AA21-131A), May 11, 2021; TSA, Security Directive Pipeline-2021-01 (May 28, 2021); and CISA, Rising Ransomware Threat to Operational Technology Assets, June 09, 2021, TSA Security Directive Pipeline-2021-02 (July 20, 2021).

¹¹ The scope of this statement did not include an evaluation of TSA's July 2021 Directive.

¹² According to TSA, pipelines are vulnerable to physical attacks—including the use of firearms or explosives—largely due to their stationary nature, the volatility of transported products, and the dispersed nature of pipeline networks spanning urban and outlying areas. Industrial control systems are typically network-based systems that monitor and control sensitive processes and physical functions, including those needed to operate pipelines.

¹³ For example, in 2015 malicious actors gained access to the business IT networks on a Ukrainian electricity utility and used that access to migrate to the utility's industrial control systems networks, which rendered some systems inoperable.

criminal groups pose the greatest cyberattack threats to U.S. critical infrastructure.¹⁴

- *Nations of concern.* China, Russia, Iran, and North Korea have the ability to launch cyberattacks that could disrupt or damage critical infrastructure, according to the Office of the Director of National Intelligence's Annual Threat Assessment. For example, China has the ability to disrupt a natural gas pipeline for days to weeks.¹⁵
- *Criminal groups.* In addition, according to the 2020 *Homeland Threat Assessment*, cybercriminals increasingly will target critical infrastructure to generate profit using ransomware by exploiting gaps in the cybersecurity of critical infrastructure entities.

These threat actors are capable of using a variety of tactics and techniques that can facilitate cybersecurity incidents that have a range of consequences. For instance, it may be possible for malicious cyber actors to manipulate, interrupt, or disrupt pipeline owner/operators' physical control processes or industrial control systems to cause disruptions:

- In the 2015 cyberattacks on the Ukrainian power grid, attackers issued unauthorized commands to open the breakers at substations that three regional electricity utilities managed, causing a loss of power to about 225,000 customers.
- In December 2019, a form of ransomware, named EKANS, infected various industrial control systems devices, reportedly in the U.S., Europe, and Japan, by encrypting files and displaying a ransom note, which impaired operations.

Recent events highlight the significant cyber threats facing the Nation's pipeline system. According to the Colonial Pipeline Company, on May 7, 2021, the company learned that it was the victim of a cyberattack. A joint alert from CISA and the Federal Bureau of Investigation (FBI) indicated that malicious actors used DarkSide ransomware against Colonial Pipeline's information technology network.¹⁶ The alert also explained that, to ensure the safety of the pipeline, the company disconnected certain industrial control systems that monitor and control physical pipeline functions so that they would not be compromised by the criminals.

According to CISA and the FBI, as of May 11, there was no indication that the DarkSide actors compromised the industrial control systems. However, disconnecting these systems resulted in a temporary halt to all pipeline operations. This in turn led to gasoline shortages throughout the southeast United States.

Federal Cybersecurity Challenges

In March 2021, we reiterated the importance of addressing four major cybersecurity challenges and 10 critical actions that the Federal government and other entities need to take to address those challenges (see fig. 1).¹⁷

¹⁴ Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (April 9, 2021). Department of Homeland Security, *Homeland Threat Assessment* (October 6, 2020).

¹⁵ Federal agencies publicly identified and characterized nation-state cyberattacks on several occasions. For example, the National Cybersecurity and Communications Integration Center and the FBI characterized Russian government actions as a multi-stage campaign targeted at small U.S. commercial facilities' networks where they gained remote access into energy sector networks. FBI and National Cybersecurity and Communications Integration Center, Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors TA18-074A (Washington, D.C.: Mar., 16 2018 (revised)). Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Jan. 29, 2019). CISA and the FBI, Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013, Alert (AA21-201A) (July 20, 2021).

¹⁶ CISA and the FBI, *DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks*, Alert (AA21-131A), May 11, 2021.

¹⁷ GAO-21-288.

Figure 1: Ten Critical Actions Needed to Address Four Major Cybersecurity Challenges

			
Establishing a comprehensive cybersecurity strategy and performing effective oversight	Securing federal systems and information	Protecting cyber critical infrastructure	Protecting privacy and sensitive data
1 Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.	5 Improve implementation of government-wide cybersecurity initiatives.	8 Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks).	9 Improve federal efforts to protect privacy and sensitive data.
2 Mitigate global supply chain risks (e.g., installation of malicious software or hardware).	6 Address weaknesses in federal agency information security programs.		10 Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.
3 Address cybersecurity workforce management challenges.	7 Enhance the federal response to cyber incidents.		
4 Ensure the security of emerging technologies (e.g., artificial intelligence and Internet of Things).			

Source: GAO analysis; images: peshkov/stock.adobe.com; Gorodenkoff/stock.adobe.com; metamorworks/stock.adobe.com; Monster Studio/stock.adobe.com. | GAO-21-105283

As we previously reported agencies need to urgently address the 10 critical actions to effectively position the Nation to prevent, or more quickly detect and mitigate the damage of, future cyberattacks. Three of these 10 critical actions are particularly relevant to pipeline security:

- *Develop and execute a more comprehensive Federal strategy for national cybersecurity and global cyberspace.* The White House's September 2018 National Cyber Strategy and the National Security Council's accompanying June 2019 Implementation Plan detailed the executive branch's approach to managing the Nation's cybersecurity. However, in September 2020, we reported that the strategy and implementation plan addressed some, but not all, of the desirable characteristics of national strategies, such as goals and resources needed.¹⁸ We recommended that the National Security Council staff work with relevant Federal entities to update cybersecurity strategy documents to include goals and resource information, among other things. The National Security Council staff neither agreed nor disagreed with our recommendation and has yet to address it.

We also highlighted the urgent need to clearly define a central role for leading the implementation of the national strategy. Accordingly, we suggested that Congress consider legislation to designate a position in the White House to lead such an effort. In January 2021, Federal law established the Office of the National Cyber Director within the Executive Office of the President.¹⁹ In April 2021, the President submitted his nomination for a National Cyber Director to the Senate for confirmation and in June 2021 the Senate confirmed the President's nominee. Moving forward, the National Cyber Director needs to either update the existing National Cyber Strategy and Implementation Plan or develop a new comprehensive strategy that addresses the desirable characteristics of national strategies.

¹⁸ GAO, *Cybersecurity: Clarity of Leadership Urgently Needed to Fully Implement the National Strategy*, GAO-20-629 (Washington, D.C.: Sept. 22, 2020).

¹⁹ The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 1752, 134 Stat. 3388, 4144 (2021).

- *Address cybersecurity workforce management challenges.* Federal and nonfederal critical infrastructure entities continue to face challenges in ensuring that their cybersecurity workforce has the appropriate skills. For example, according to a 2019 assessment from the Department of Energy, the electricity subsector continues to face challenges in recruiting and maintaining experts with strong knowledge of cybersecurity practices, as well as knowledge of industrial control systems supporting the electric grid.²⁰ Further, we reported in October 2020 that the Federal Aviation Administration does not currently have a staff training program specific to avionics cybersecurity and none of the agency's certification staff are required to take cybersecurity training tailored to their oversight roles.²¹ Until these challenges are resolved, Federal and nonfederal critical infrastructure entities may not have the expertise necessary to address the increasing cybersecurity risks to their systems.
- *Strengthen the Federal role in protecting the cybersecurity of critical infrastructure.* Since 2010, we have made nearly 80 recommendations for various Federal agencies to enhance infrastructure cybersecurity. For example, in February 2020, we recommended that agencies better measure the adoption of the National Institute of Standards and Technology (NIST) framework of voluntary cyber standards and correct sector-specific weaknesses.²² However, as of December 2020, most of these recommendations (nearly 50) have not been implemented. As a result, the risks of unprotected infrastructures being harmed are heightened.

Pipeline Stakeholders' Security Roles and Responsibilities

Protecting the Nation's pipeline systems is a responsibility shared by both TSA and private industry stakeholders. TSA's Pipeline Security Branch conducts voluntary security reviews of the privately owned and operated pipelines, among other activities. These reviews—Corporate Security Reviews (CSR) and Critical Facility Security Reviews (CFSR)—assess the extent to which the 100 most critical pipeline systems are following the intent of TSA's Pipeline Security Guidelines.²³ CSRs are voluntary on-site reviews of a pipeline owner's corporate policies and procedures. CFSRs are voluntary on-site inspections of critical pipeline facilities, as well as other selected pipeline facilities, throughout the Nation (see fig. 2).

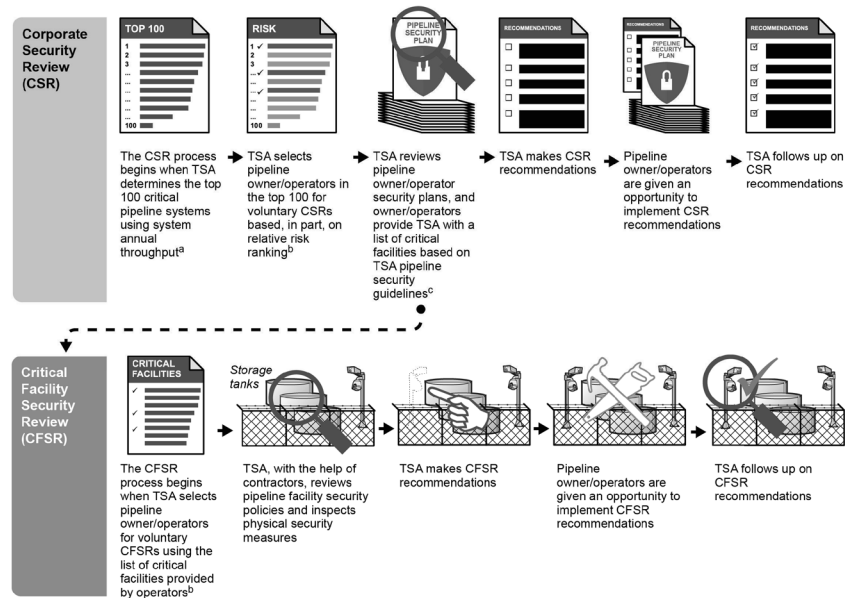
²⁰ GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid*, GAO-19-332 (Washington, D.C.: Aug. 26, 2019).

²¹ GAO, *Aviation Cybersecurity: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks*, GAO-21-86 (Washington, D.C.: Oct. 9, 2020).

²² GAO, *Critical Infrastructure Protection: Additional Actions Needed to Identify Framework Adoption and Resulting Improvements*, GAO-20-299 (Washington, D.C.: February 25, 2020).

²³ TSA initially identifies the 100 highest risk pipeline systems based on the amount of material transported through the system. Subsequently, pipeline owner/operators are to use criteria in the Guidelines to self-identify the critical facilities within those higher risk systems and report them to TSA. TSA's Pipeline Security Branch then conducts CFSRs at the critical facilities identified by pipeline owner/operators. However, in December 2018 we reported that our analysis of TSA's data found that at least 34 of the top 100 critical pipeline systems TSA deemed highest risk indicated that they had no critical facilities. GAO-19-48.

Figure 2: Overview of the Transportation Security Administration's (TSA) Voluntary Security Review Process with Pipeline Owner/Operators



Source: GAO analysis of TSA information. | GAO-21-105263

^aTSA uses system annual throughput in determining the top 100 critical pipeline systems, which is based on the amount of hazardous liquid or natural gas product transported through a pipeline in 1 year.

^bBecause of the voluntary nature of TSA's pipeline security program, TSA requests selected operators to participate in its pipeline security reviews—the CSR and CFSR.

^cUnder TSA's Pipeline Security Guidelines, pipeline operators are to self-identify the critical facilities within their pipeline system and report their critical facilities to TSA.

Following the Colonial Pipeline cyberattack, TSA issued Security Directive Pipeline-2021-01 effective for one year beginning May 28, 2021 requiring certain pipeline owner/operators to take specific actions to enhance pipeline cybersecurity.²⁴ In this May 2021 Directive, TSA requires, among other things, certain pipeline owner/operators to report cybersecurity incidents to DHS. The Directive also requires pipeline owner/operators to designate a cybersecurity coordinator and review current activities against TSA's recommendations for pipeline cybersecurity to assess cyber risks, identify any gaps, develop remediation measures, and report the results to TSA and DHS.²⁵

In July 2021, TSA issued Security Directive Pipeline-2021-02: *Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing* effective for one year beginning July 26, 2021.²⁶ In this July 2021 Directive, TSA establishes requirements for certain pipeline owner/operators to implement cybersecurity mitigation measures; develop a cybersecurity contingency and recovery plan; and undergo an annual cybersecurity architecture design review, among other things.

TSA Has Addressed Several Previously Identified Weaknesses in the Management of Pipeline Security

Our December 2018 and June 2019 reports identified several weaknesses in TSA's pipeline security program and made 15 recommendations to address them (see app. D). TSA has taken actions to address several weaknesses in the management of pipeline security and has fully addressed 12 of our recommendations related to four areas. Specifically, TSA has clarified its pipeline security guidelines, improved per-

²⁴TSA Security Directive Pipeline-2021-01 (May 28, 2021).

²⁵TSA recommendations for pipeline cybersecurity are based on Section 7 of the Guidelines, which describe security measures for pipeline cyber assets.

²⁶TSA Security Directive Pipeline-2021-02 (July 20, 2021).

formance monitoring, assessed staffing needs, and updated guidance on Federal roles and responsibilities:

- *Clarified pipeline security guidelines.* In December 2018, we found that TSA had revised the Pipeline Security Guidelines in March 2018, but had not established a documented process to ensure that revisions regularly occur and to fully capture updates to supporting standards and guidance. For example, while TSA revised its guidelines in March 2018 to incorporate cybersecurity principles and practices from the NIST Cybersecurity Framework, the revisions did not incorporate cybersecurity elements that NIST added to the latest Cybersecurity Framework the following month in April 2018, such as the Supply Chain Risk Management category. We also found that TSA did not specify clear criteria for pipeline owner/operators to use in determining critical facilities.

In our December 2018 report, we recommended that TSA implement a documented process for reviewing and revising its Pipeline Security Guidelines, as well as clarify these Guidelines by defining key terms within its criteria for determining critical facilities. In March 2019, TSA officials established a documented internal operating procedure for reviewing all of TSA's surface transportation security guidance annually, which include its Pipeline Security Guidelines, and updating it at least once every 5 years or earlier if TSA determines that new or revised guidance is in the public interest. According to TSA officials, in December 2020, TSA also clarified critical facility criteria by using existing regulatory terminology, among other clarifications. These actions addressed our recommendations.

- *Improved performance monitoring.* In December 2018, we found that TSA developed three databases to track CSR and CFSR recommendations and their implementation status. Also, while TSA used a database to track CFSR recommendations, we found that TSA had not tracked the status of CSR recommendations for security improvements in over 5 years. We recommended that TSA take steps to enter information on CSR recommendations and monitor and record their status. In April 2020, TSA reported that it began updating and monitoring CSR recommendations in its database.
- *Assessed staffing needs.* In December 2018, we also found that TSA had not established a workforce plan for its Pipeline Security Branch that identified staffing needs or cybersecurity skills required to best implement security reviews, such as CSRs and CFSRs. We recommended that TSA develop a strategic workforce plan that outlines the knowledge, skills, and abilities, including those related to cybersecurity, needed to effectively conduct pipeline security reviews. TSA completed the Workforce Assessment Report in May 2021. The Assessment Report identified, among other things, several staffing inadequacies, particularly related to the pipeline cybersecurity mission. Specifically, the Assessment Report highlighted that the organization lacks qualified personnel with relevant skills, appropriate certifications, or expertise in cybersecurity and that over one-third of the agency's position descriptions were improperly classified for the duties required.

TSA's Assessment Report also noted that TSA is short the necessary positions to perform the current and projected pipeline security mission, with a 41 percent increase in staffing needed to position the organization for mission success.²⁷ The assessment includes a recommended workforce plan that defines short-term and long-term initiatives for addressing the staffing inadequacies. For example, the recommended workforce plan lists initiatives for developing and codifying specific duties required for physical or cybersecurity, budgeting to fund new staff position requirements, and collaborating with TSA's Human Capital office to recruit and hire needed staff. These actions help ensure that TSA is able to meet its mission of reducing pipeline systems' vulnerabilities to physical and cybersecurity risks, especially in a dynamic and evolving threat environment.

- *Updated guidance for Federal pipeline security roles.* We reported in June 2019 on the need for key pipeline security documents to reflect the current operating environment. Specifically, in 2006, TSA and the Department of Transportation's Pipeline and Hazardous Materials Safety Administration (PHMSA) signed an annex to a memorandum of understanding to further delineate their pipeline se-

²⁷ According to TSA officials, the Pipeline Security Branch employed 34 staff as of June 2021.

curity-related responsibilities.²⁸ We found that the memorandum of understanding had not been reviewed to consider pipeline security developments since its inception and did not fully reflect the agencies' pipeline security and safety activities. Consequently, we recommended that the TSA and PHMSA Administrators revise the annex, to include a provision requiring periodic reviews of, and corresponding updates to, the memorandum of understanding. As of February 2020, TSA and PHMSA had addressed these recommendations by including a provision in the memorandum of understanding that committed the agencies to reviewing it at least once every 5 years.²⁹

TSA Has Not Fully Addressed Two Previously Identified Pipeline Cybersecurity-Related Weaknesses

TSA has not fully addressed two key pipeline cybersecurity-related weaknesses we previously identified. These weaknesses include: (1) incomplete information for pipeline security risk assessments and (2) aged protocols for responding to pipeline security incidents. These weaknesses correspond to three of the 15 recommendations from our December 2018 and June 2019 reports.

Incomplete Information for Pipeline Security Risk Assessments

In December 2018, we reported that TSA had incomplete information for pipeline security risk assessments. We reported the Pipeline Security Branch had developed a risk assessment model that combines all three elements of risk—threat, vulnerability, and consequence—to generate a risk score for pipeline systems. The Pipeline Security Branch developed the Pipeline Relative Risk Ranking Tool in 2007 for use in assessing various security risks to the top 100 critical pipeline systems based on volume of material transported through the system (throughput).³⁰

The risk ranking tool calculates threat, vulnerability, and consequence for each pipeline system on variables such as the amount of throughput in the pipeline system and the number of critical facilities. According to TSA at the time of our review, it collected these data from pipeline owner/operators, as well as other Federal agencies such as the departments of Transportation and Defense. The risk ranking tool then generates a risk score for each of the 100 most critical pipeline systems and TSA uses the risk scores to prioritize its pipeline security assessments.

We made four recommendations to improve TSA's risk ranking tool in our December 2018 report. TSA implemented two of the recommendations but, as of June 2021, has not fully addressed the remaining two (see app. I).³¹ One recommendation TSA has not fully addressed is that it identify or develop data sources relevant to threat, vulnerability, and consequence, and incorporate that data into the Pipeline Relative Risk Ranking Tool. Such data sources could include information not tracked by TSA as of our December 2018 report, such as data on cybersecurity threats, prior attacks, natural hazards, physical pipeline condition, and cross-sector interdependencies.³² TSA also has not yet conducted a peer review of its risk ranking tool, as we recommended. TSA stated that doing so was contingent on first enhancing the tool in accordance with our other open recommendation. Addressing these recommendations is important, as developing this information and incorporating it into the risk ranking tool would provide more assurance that the Pipeline Security Branch ranks relative risk among pipeline systems using comprehensive and accurate data.

²⁸ Department of Transportation's PHMSA regulates the safety of pipelines operating within the United States.

²⁹ The update also included several clarifications for how TSA and PHMSA are to coordinate, such as lines of authority and responsibility for interagency incident information sharing.

³⁰ According to DHS, a risk assessment is a product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision-making. A risk assessment is also considered the appraisal of the risks facing an entity, asset, system, network, geographic area or other grouping.

³¹ TSA implemented our recommendations to (1) update the Pipeline Relative Risk Ranking Tool to include up-to-date data to ensure it reflects industry conditions, including throughput and threat data; and (2) document the data sources, underlying assumptions, and judgments that form the basis of the Pipeline Relative Risk Ranking Tool, including sources of uncertainty and any implications for interpreting the results from the assessment.

³² Cross-sector interdependencies, as described in the 2013 National Infrastructure Protection Plan, concerns how infrastructure sectors interact, including through reliance on shared information and communications technologies (e.g., cloud services) and how that interaction shapes how the Nation's critical infrastructure partners should collectively manage risk. For example, all critical infrastructure sectors rely on functions provided by energy, communications, transportation, and water systems, among others. In addition, interdependencies flow both ways, as with the dependence of energy and communications systems on each other and on other functions.

Aged Protocols for Responding to Pipeline Security Incidents

In June 2019, we reported that TSA had not reviewed or revised its 2010 Pipeline Security and Incident Recovery Protocol Plan to ensure it addressed changes in at least three key areas.³³ The 2010 plan's stated intent is to establish a comprehensive interagency approach to counter risks, coordinate Federal agencies' actions, and minimize the consequences of incidents involving pipeline infrastructure as well as recovery time from them.³⁴ The plan also defines the roles and responsibilities of Federal agencies; tribal, state, and local governments; and the private sector during a pipeline incident and the measures they may take related to pipeline infrastructure security incidents. According to the plan, TSA, PHMSA, the Department of Energy, and the Federal Bureau of Investigation have principal roles in pipeline incident response, while other agencies such as the U.S. Coast Guard and the Federal Emergency Management Agency have supporting roles. TSA's plan states that it will be updated periodically to address changes in pipeline security threats, technology, and Federal laws and policies. However, we reported in June 2019 that TSA had not reviewed or revised its 2010 plan to ensure it addresses changes in at least three key areas: cybersecurity-related laws and policies, Federal incident management policies for pipeline stakeholders, and DHS's terrorism alert system.

Representatives of the four pipeline associations we interviewed at the time of our June 2019 report told us that their membership more clearly understood Federal agencies' roles and responsibilities related to physical incidents than to cybersecurity. All of these associations' representatives told us that the process for reporting a cyber incident was less clear because, in part, of the large number of Federal agencies with a cybersecurity-related role. Further, they indicated that clarifying the cybersecurity roles and responsibilities of the Department of Energy, Federal Energy Regulatory Commission, and TSA would improve owner/operators' ability to appropriately report and respond to a cyber incident.

We recommended that TSA periodically review and, as appropriate, update the 2010 Pipeline Security and Incident Recovery Protocol Plan to ensure the plan reflects relevant changes in pipeline security threats, technology, Federal law and policy, and any other factors relevant to the security of the Nation's pipeline systems. According to TSA officials as of May 2021, TSA completed a review of the plan and determined that updates are needed and will require coordination with other agencies. Fully addressing our recommendation will better ensure that Federal agencies' actions are well-coordinated in response to a pipeline-related physical or cyber incident, and that pipeline stakeholders understand Federal agencies' roles and responsibilities in helping pipeline owner/operators to restore service after a pipeline-related physical or cyber incident.

TSA's Pipeline Security Directives Mandate Mitigation Strategies for Cyber Threats

TSA's May 2021 Directive requires certain pipeline owner/operators to take three specific actions—report cybersecurity incidents to DHS, designate a cybersecurity coordinator, and review their current activities against the Pipeline Cyber Asset Security Measures in TSA's Pipeline Security Guidelines. It directs these pipeline owner/operators to assess whether their current operations and activities to address cyber risks are consistent with the Guidelines, identify any gaps, develop remediation measures, and report the results to TSA and CISA by the end of June 2021.³⁵

TSA's July 2021 Directive mandates that certain pipeline owner/operators implement cybersecurity mitigation measures; develop a cybersecurity contingency and recovery plan in the event of an incident; and undergo an annual cybersecurity architecture design review, among other things.³⁶ According to TSA, the July 2021 Di-

³³ GAO-19-426.

³⁴ The plan defines a pipeline security incident as any event determined by DHS or TSA to be significant enough to warrant monitoring. Such an event could be an occurrence, natural or manmade, requiring a response to protect life or property, including major disasters, emergencies, terrorist attacks, terrorist threats, civil unrest, wild land and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, tsunamis, war-related disasters, public health and medical emergencies, and other occurrences requiring an emergency response.

³⁵ TSA Security Directive Pipeline-2021-01 (May 28, 2021). The Directive calls for owner/operators to report assessment results using a TSA-provided form that, once completed, is protected as sensitive security information.

³⁶ TSA Security Directive Pipeline-2021-02 (July 20, 2021).

rective was developed in consultation with CISA to include many of the cybersecurity mitigation measures noted in recent security alerts.³⁷

TSA's recent security directives are important requirements for pipeline owner/operators, because the agency's Pipeline Cyber Asset Security Measures in its Pipeline Security Guidelines do not include several known mitigation strategies for current cyber threats, including ransomware attacks.³⁸ In June 2021, TSA officials told us that a timely update to address current cyber threats is appropriate and said that they anticipate updating the Guidelines over the subsequent year. Officials stated that time is needed to consult with a wide range of industry stakeholders before finalizing the update.

Chair Cantwell, Ranking Member Wicker, and Members of the Committee, this completes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

APPENDIX I: STATUS OF SELECTED GAO RECOMMENDATIONS TO STRENGTHEN TRANSPORTATION SECURITY ADMINISTRATION (TSA) OVERSIGHT OF PIPELINES

Table 1: Status of Selected GAO Recommendations to Strengthen Transportation Security Administration (TSA's) Oversight of Pipelines, through June 2021

GAO recommendation	Status of recommendation and actions needed if not fully implemented
<i>Actions needed to address significant weaknesses in TSA's pipeline security program management</i>	
Implement a documented process for reviewing, and if deemed necessary, for revising TSA's Pipeline Security Guidelines at regular defined intervals. (GAO-19-48) ^a	Recommendation implemented.
Clarify TSA's Pipeline Security Guidelines by defining key terms within its criteria for determining critical facilities. (GAO-19-48) ^a	Recommendation implemented.
Develop a strategic workforce plan for TSA's Security Policy and Industry Engagement's Surface Division, 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, that are needed to effectively conduct Corporate Security Reviews (CSR) and Critical Facility Security Reviews (CFSR). (GAO-19-48) ^a	Recommendation implemented.
Update the Pipeline Relative Risk Ranking Tool to include up-to-date data to ensure it reflects industry conditions, including throughput and threat data. (GAO-19-48) ^a	Recommendation implemented.
Fully document the data sources, underlying assumptions and judgments that form the basis of the Pipeline Relative Risk Ranking Tool, including sources of uncertainty and any implications for interpreting the results from the assessment. (GAO-19-48) ^a	Recommendation implemented.

³⁷ NSA and CISA, *NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems*, Alert (AA20-205A), July 23, 2020. CISA and the Federal Bureau of Investigation (FBI), *DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks*, Alert (AA21-131A), May 11, 2021; TSA, *Security Directive Pipeline-2021-01* (May 28, 2021); and CISA, *Rising Ransomware Threat to Operational Technology Assets*, June 09, 2021, TSA Security Directive Pipeline-2021-02 (July 20, 2021).

³⁸ The scope of this statement did not include an evaluation of TSA's July 2021 Directive. However, our preliminary observations indicate that this security directive is placing significant additional cybersecurity requirements on private sector pipeline owner/operators and additional oversight will be important going forward.

Table 1: Status of Selected GAO Recommendations to Strengthen Transportation Security Administration (TSA's) Oversight of Pipelines, through June 2021—Continued

GAO recommendation	Status of recommendation and actions needed if not fully implemented
Identify or develop other data sources relevant to threat, vulnerability, and consequence consistent with the National Infrastructure Protection Plan and Department of Homeland Security (DHS) critical infrastructure risk mitigation priorities and incorporate that data into the Pipeline Relative Risk Ranking Tool to assess relative risk of critical pipeline systems, which could include data on prior attacks, natural hazards, feedback data on pipeline system performance, physical pipeline condition, and cross-sector interdependencies. (GAO-19-48) ^a	Not fully implemented. DHS stated that TSA will incorporate that data into the Pipeline Risk Ranking Tool to assess relative risk of critical pipeline systems, which could include data on prior attacks, natural hazards, feedback data on pipeline system performance, physical pipeline condition, and cross-sector interdependencies. Identifying or developing other sources relevant to threat, vulnerability, and consequence consistent with the National Infrastructure Protection Plan and DHS critical infrastructure risk mitigation priorities, and incorporating it into the risk ranking tool, would provide more assurance that TSA ranks relative risk among pipeline systems using comprehensive and accurate data.
Coordinate an independent, external peer review of TSA's Pipeline Relative Risk Ranking Tool, after the Pipeline Security Branch completes enhancements to its risk assessment approach. (GAO-19-48) ^a	Not fully implemented. DHS stated that, after completing enhancements to its risk assessment approach, TSA will take steps to coordinate an independent, external peer review of its Pipeline Relative Risk Ranking Tool. Better considering threat, vulnerability, and consequence elements in its risk assessment and incorporating an independent, external peer review in its process would provide more assurance that the Pipeline Security Branch ranks relative risk among pipeline systems using comprehensive and accurate data and methods.
Ensure that TSA has a suite of performance measures which exhibit key attributes of successful performance measures, including measurable targets, clarity, and baseline and trend data. (GAO-19-48) ^a	Recommendation implemented.
Take steps to enter information on CSR recommendations and monitor and record their status. (GAO-19-48) ^a	Recommendation implemented.
Improve the quality of TSA's pipeline security program data by developing written documentation of its data entry and verification procedures, implementing standardized data entry formats, and correcting existing data entry errors. (GAO-19-48) ^a	Recommendation implemented.
<i>Key pipeline security documents need to reflect current operating environment</i>	
Work with the Pipeline and Hazardous Materials Safety Administration (PHMSA) Administrator to develop and implement a timeline with milestone dates for reviewing and, as appropriate, updating the 2006 MOU Annex. (GAO-19-426) ^b	Recommendation implemented. ^c
In consultation with the PHMSA Administrator, revise the 2006 MOU Annex to include a provision requiring periodic reviews of, and as appropriate, corresponding updates to the Annex. (GAO-19-426) ^b	Recommendation implemented. ^c
Periodically review, and as appropriate, update the 2010 Pipeline Security and Incident Recovery Protocol Plan to ensure the plan reflects relevant changes in pipeline security threats, technology, Federal law and policy, and any other factors relevant to the security of the Nation's pipeline systems. (GAO-19-426) ^b	Not fully implemented. As of June 2021, TSA officials reported that they completed a review of the Pipeline Security Incident Recovery Protocol Plan and determined that updates are needed. The updates require additional coordination with PHMSA as well as internal review within TSA, according to TSA officials. By periodically reviewing and, as appropriate, updating its plan, TSA could better ensure it addresses changes in pipeline security threats and Federal law and policy related to cybersecurity, incident management and DHS's terrorism alert system, among other things. TSA could also provide greater assurance that pipeline stakeholders understand Federal roles and responsibilities related to pipeline incidents, including cyber incidents, and that response efforts to such incidents are well-coordinated.

Source: GAO. | GAO-21-105263

^aCritical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management, GAO-19-48 (Washington, D.C.: December 18, 2018).

^bCritical Infrastructure Protection: Key Pipeline Security Documents Need to Reflect Current Operating Environment, GAO-19-426 (Washington, D.C.: June 5, 2019).

^cThis recommendation was also implemented by PHMSA, in coordination with TSA.

The CHAIRMAN. Thank you, Ms. Gordon, and again thanks to all the witnesses for their testimony.

I want to also mention that Senator Wicker and I today are sending a letter to the Secretary of Commerce about the need to upgrade and identify information and proprietary information critical to our security system.

The nation's reliance on cyber-enabled systems demands that the Department of Commerce, including the National Institute of Standards and Technology, deepen its critical role in protecting the Nation from cybersecurity threats vulnerability and funding that matches the seriousness of this threat. So flat funding of the Department of Commerce cybersecurity efforts while growing the agency's budget, as reflected in the President's request, is insufficient to meet these needs. So we'll be sending that to the Department of Commerce today.

One of the things I wanted to mention—I also wanted to enter one thing I didn't enter into the record was a—I love it when we have bipartisan efforts—Cybersecurity Rules Needed for Pipelines by FERC Commissioners Neal Chatterjee and Richard Glick, shows you that this issue, along with that GAO report, has been showing since 2018 that we have a serious problem here and now we have the Colonial Pipeline as a very loud example.

[The information referred to follows:]

COLONIAL PIPELINE CYBER ATTACK HIGHLIGHTS NEED FOR MORE SERIOUSNESS IN ENERGY POLICY

By David Blackmon, Senior Editor—May 13, 2021 9:21am EDT



WASHINGTON, DC—MAY 11: Secretary of Energy Jennifer Granholm briefs reporters on the cyber attack . . . [+] GETTY IMAGES

With Colonial Pipeline now in the process of *being restarted*, we can hope that the major *disruptions to gasoline supply* and resulting spikes in gas prices in the 17 states the system serves will be relieved in a matter of days. The danger in that potentially happy outcome resides in the possibility that appropriate concerns about the security of critical infrastructure in the U.S. will dissipate along with the disruptions.

Colonial is unique in the scale and scope of its service area and volume of deliveries. No other U.S. pipeline can say it delivers 45% of total gasoline supplies across

17 states on a daily basis. But it is also a vital part of a highly-interconnected national gasoline transportation network in which major disruptions in one segment can ultimately result in nationwide impacts to consumers and the economy.

Think of the nation's gasoline transportation network in the same way we think of an electrical power grid. The loss of significant generation capacity in one segment of a power grid can result in system-wide blackouts as power is diverted from other parts of the grid to fill in the void. Had the Colonial outage lingered for weeks instead of mere days, we could have seen the same kind of domino effect across the national transportation and delivery network. We know this because we have seen it happen related to major, long-term pipeline outages in the past.



Motorists line up at an EXXON station selling gas at \$3.29 per gallon soon after it's fuel supply . . . [+] AFP VIA GETTY IMAGES

The U.S. pipeline infrastructure system is vulnerable to terrorist attack, and make no mistake about it, the group that appeared to take credit for the Colonial attack is a group of terrorists. The fact that the U.S. legal system is so inept at dealing with this kind of terrorism and so rarely exacts any form of harsh punishment for such actions belies a lack of seriousness in addressing what is a growing problem.



WASHINGTON, DC—MAY 10: Deputy National Security Advisor for Cyber and Emerging Technology Anne . . . [+] GETTY IMAGES

The same applies to the Biden/Harris administration's posturing towards the pipeline business in general. Much has been made of statements made by two administration officials this week in reaction to the Colonial situation.

On Monday, Anne Neuberger, deputy national security advisor for cyber and emerging technologies, *when asked* by White House reports a about whether Colonial would consent to the terrorists' ransom demand, said "Typically that's a private sector decision . . . We recognize that victims of cyberattacks often face a very difficult situation and they have to just balance often the cost-benefit when they have no choice with regards to paying a ransom. Colonial is a private company and we'll defer information regarding their decision on paying a ransom to them," Neuberger said. *[Note: A report at Bloomberg on May 13 indicates that the company did pay \$5 million in ransom to the terrorist group.]*

Then on the next day, Energy Secretary Jennifer Granholm *admitted* during another White House press briefing that "pipe is the best way" to transport fuel. While both statements by both senior officials are obviously correct, it is legitimate to ask where their voices were on January 20, when their President cancelled the Keystone XL Pipeline project.

The decision by *TC Energy* to build *Keystone XL* was after all a private sector decision based on a cost-benefit analysis related to market demand for such a pipeline's services. The alternative to Keystone XL is to move the Canadian crude oil it would transport to market on thousands of trucks and many trains every day, obviously less safe and more environmentally impactful ways of moving fuel.

Yet, despite the fact that TC Energy had met and even exceeded the regulatory and permitting requirements across two different presidential administrations, and despite the fact that the private company had already invested billions of dollars and constructed hundreds of miles of the line itself by January 20, President Biden cancelled all of that, along with thousands of high-paying blue-collar jobs, with the stroke of a pen during his first day in office.

The stark dichotomy of logic surrounding this administration's decision-making related to Colonial and Keystone XL belies a lack of seriousness in and highly-charged political nature of the choices it makes in the energy space.

America's news and entertainment media today are filled with hopes and dreams about an all-renewable energy future materializing somewhere down the road, and that's great. In the meantime, though, Americans still need to get to work and take their kids to school each day, and *99% of them* are doing that in automobiles powered by gasoline and diesel fuel. That heavy reliance on gasoline and diesel-fueled cars is likely to predominate for decades to come, and that means America will have to continue building and maintaining pipelines across those decades.

When it comes to energy policy and the nation's critical pipeline infrastructure, Americans deserve a little more seriousness and consistency than they have received thus far from this presidential administration.

Cyber security rules needed for pipelines: FERC commissioners

Neil Chatterjee, Richard Glick, Federal Energy Regulatory Commission
June 18, 2018 Updated: June 18, 2018 8:04 a.m.

Associated Press

If you have turned on the news or picked up a paper lately, you have probably seen reports that foreign enemies are increasingly launching cyber-attacks on America's critical infrastructure, including energy facilities. To address these threats, electric grid operators must comply with mandatory standards overseen by the Federal Energy Regulatory Commission (FERC) that protect against cyber and other attacks that threaten the reliability of our electric service.

Natural gas pipelines are not subject to similar standards. But given the increasing threats we face, the time has come to establish them for natural gas pipelines.

Abundant and affordable natural gas has facilitated a major shift in the United States' electric generation mix. The emergence of natural gas as a significant part of the fuel mix has greatly raised the stakes for pipeline cyber security.

Although FERC has the authority to issue certificates for new interstate gas pipelines and set their rates, the Commission does not have responsibility for pipeline security. That charge falls to the Transportation Security Administration, the same agency that is responsible for overseeing the security of 851 million aviation passengers per year, 138,000 miles of railroad track, and 4 million miles of highway.

In May 2017, TSA confirmed that it had just six full-time employees to oversee the security of the more than 2.7 million miles of natural gas, oil, and other hazardous liquid pipelines that traverse the country. In addition, although it has the authority to enforce mandatory standards to protect gas pipeline infrastructure from cyber-attacks, TSA has chosen to rely, instead, on voluntary standards.

Natural gas pipelines have a long history of providing reliable service. But given our growing dependence on natural gas in conjunction with the escalating potential for cyber-attacks, we cannot simply hope for the best.

<https://www.chron.com/business/energy/article/Cyber-security-rules-needed-for-pipelines-FERC-13002008.php>

In our view, Congress should vest the responsibility for pipeline security with an agency that fully comprehends the nation's energy sector and has sufficient resources to address the growing cyber security threat to gas pipelines. As the Sector-Specific Agency for energy security, the Department of Energy could be an appropriate choice. Such a move would be particularly timely given the Energy Department's recent announcement that it will be forming an office specifically focused on cybersecurity.

Regardless of where Congress vests this responsibility, the regulator must have the statutory authority, resources, and commitment to implement mandatory cybersecurity standards for gas pipelines. We will be the first to admit that mandatory standards are not a panacea.

The Commission has overseen the implementation of mandatory cyber security standards for the electric grid for over a decade, and there have been many challenges and lessons learned along the way. Mandatory standards for gas pipelines need not be identical to those used by the electric sector and should instead reflect the unique operational risks facing gas pipelines.

Nor are mandatory standards sufficient to ensure the cybersecurity of natural gas pipelines. But they can form an important foundation that individual utilities can build upon through voluntary initiatives such as promoting best practices and sharing threat intelligence.

There are few issues on which individuals from both sides of the aisle can find common ground. But the safety and security of our electric grid is an area that should rise above partisan politics. We will continue evaluating energy security in a thoughtful and bipartisan manner, and we encourage our colleagues in Congress and other agencies to do the same.

America's energy consumers depend upon it.

Neil Chatterjee, a Republican, is chairman of the Federal Energy Regulatory Commission. Richard Glick, a Democrat, was confirmed to the commission by the Senate in November, following his nomination by President Trump.

The CHAIRMAN. So I guess I just want to start with something very basic here because you guys talked a lot about interagency coordination. I'm not sure that Americans are really interested in, you know, our internal interagency coordination. What they're interested in is critical infrastructure being protected.

So one of the things that I feel here is that the complexity of this issue is getting away from us a little bit in the context of it is very complex and the demands of cybersecurity are very complex. They're not too complex not to implement, but they are very complex and I have a feeling that we're not keeping pace with some of these solutions.

If the witnesses would answer do you think that that's the case? What do you think we need to do to better implement cybersecurity solutions so that we can move forward?

Mr. PEKOSKE. Chair Cantwell, I agree with your comment and certainly, you know, cyber moves fast and changes very quickly. We need to keep pace with that.

We try to tie our requirements to NIST standards and NIST keeps—you know, NIST is pretty much state-of-the-art with respect to cybersecurity in our view.

The other thing that I feel is very, very important here, as you mentioned, this is an ecosystem, it's very interconnected, is to stay very connected and very collaborative with our private sector partners, and I use that partner term intentionally because, you know, we're only going to be successful here if this partnership is successful.

The other thing I would highlight is that Surface Transportation Security Advisory Committee, which includes owners and operators across surface transportation and agency representatives, and so that gives us a good opportunity to come together and to look at the issues facing surface and pipelines and figure out the best way to move forward.

So I think we have mechanism in place to do that. The key, though, is going to be key coordination and communication amongst all parties.

The CHAIRMAN. Ms. Trottenberg.

Ms. TROTTEMBERG. I'll just add a bit to what the Administrator said.

No question obviously in the transportation field, as in so many others, the technological advances are extraordinary, you know. Again, as I discussed in my testimony, in terms of, you know, the remarkable operational systems we now have in pipelines, we're seeing in vehicles, sort of across a lot of our different modes.

I think the Administrator put it well. We are, you know, as an agency now, I think, trying to work ever more closely with TSA, with CISA, with our White House partners, and to have that partnership with industry. You know, as we move forward in this more technological age, we are going to need to be, you know, as you were pointing out, Chair Cantwell, very, very cutting edge, very nimble, and very collaborative.

The CHAIRMAN. Ms. Gordon.

Ms. GORDON. I think you're exactly right, Chair Cantwell. This is a dynamic environment and one where the threats are almost unknowable at times.

GAO has three open recommendations still for the TSA. One of them is to develop additional data sources, beyond what they're drawing on from the private sector, to better understand and rank their priority pipeline systems and so we are looking for them to add additional data sources to their priority relative ranking tool and those might include cyber threats, prior attacks, the physical condition of the pipelines themselves, and inter-sector, interdependencies.

The CHAIRMAN. So what do you—I mean, I just don't think for the American public and the vulnerability that Colonial laid bare to all of us, people just want to hear more about, you know, the need for this interagency coordination.

What do you think we need to do to get technology implemented faster?

Ms. GORDON. GAO has over 950 open recommendations about cybersecurity Federal Government-wide. We've put out 3,700 recommendations on cybersecurity for the Federal Government since 2010 and 950 remain open.

The CHAIRMAN. So I will turn to my colleague here because I see my time has expired, but many people will see I was very aggressive with the Trump Administration about this. I plan to be very aggressive with the Biden Administration about this, as well. This is just not acceptable after the Colonial Pipeline. It wasn't acceptable before but now we know how serious the threat can be and the challenges that we face are really, you know, as I have mentioned the *New York Times* clip, now people know, now people know, and so we have to do better.

I'll turn to my colleague, but I'm sure he has spent many hours in the skiff. I've spent many hours in the skiff on this issue. There are things that can be done. We should be doing them now.

Senator Wicker.

Senator WICKER. I'm astounded by the hundreds of open recommendations that you mentioned.

Are they overlapping? I'm just—I can't conceive of that. I'm even reluctant to ask you to supplement the record by sending them all to us.

Ms. GORDON. We've been reporting on cybersecurity as a high-risk issue for a number of years. So they span a decade, 11–12 years of work right now.

They focus in on four major challenges that the Federal Government faces which are developing a comprehensive cyber strategy, securing Federal systems and information, protecting cyber-critical infrastructure, what we're talking about today, and protecting privacy and sensitive data. So those are the four major challenges for cybersecurity that GAO has reported on.

Senator WICKER. OK. Well, let's talk about the Security Directive done just a month or two ago, this year, and then a second Security Directive on July 20th, just a day or two ago. This was done without traditional rulemaking process, such as notice and comment.

Ms. Gordon, we can go back this way, is that a problem at all? What observations do you have about that shortcut? Was it necessary, and what advice can you give us?

Ms. GORDON. TSA has the authority to regulate in this space. TSA has the authority to regulate transportation modes. So they

were well within their authorities to issue the May Directive and it was a step toward gathering additional information that the agency may need about the status of the security of the pipelines.

Senator WICKER. Do you think us stakeholders' viewpoints were heard during this necessarily hurried-up process?

Ms. GORDON. I have no way to know that.

Senator WICKER. Anybody else want to comment?

Mr. PEKOSKE. Yes, Senator. The stakeholder concerns were heard throughout the entire process.

I would suggest that the Security Directive process actually enables the flexibility and agility, Chair Cantwell, that you talked about. To go through a rulemaking process is a lengthy process.

Security directives can be implemented immediately and then once a security directive is implemented with that coordination in advance, it doesn't mean that industry had all the things that they wanted or wanted out of a security directive, but we considered their input, we issue it, and then we have a procedure within the security directive regime that allows an affected industry partner to say, hey, I see your requirement here, I see what security outcome you're trying to achieve. I've got a better way to do that and that also keeps us on the leading edge of cybersecurity.

So the industry representative will submit that alternative procedure to us. We will rapidly review it and provide them an answer back. So there is a lot of flexibility and speed built into the security directive process.

Additionally, the security directives are traditionally when they're first issued oftentimes issued for a year. They can be renewed in increments following that or we can follow another process to actually go through a formal notice and comment rulemaking. We haven't determined what the path ahead is for that in the longer term, but, you know, I just look at Colonial.

I don't think anybody could have acted faster than we did with our Security Directive authority and given that the requirements we placed on the industry were consistent with NIST cybersecurity framework requirements and consistent with our pipeline security guidelines, which the industry helped us build, there really weren't a lot of surprises in my view there. It's just the scope and the speed.

Finally, I would submit that speed is really important here. Senator, you know, —

Senator WICKER. Well, let me just interject and perhaps you can supplement that answer.

I agree with you. I think government should be nimble in situations like this and I know there has been a frustration on this side of the dais that government is quite often slow and creaky. So I commend you for that.

Let me just ask does anybody want to comment about the possibility of condemning China for cyber attacks but not imposing sanctions, to actually impose consequences on China? Would someone like to comment on that?

Mr. PEKOSKE. I would just offer that, you know, this is a long-term process and imposing sanctions on a foreign power is not something as an agency administrator that I would have independent authority to do, but certainly the National Security Coun-

cil process, irregardless of Administration, that is where those issues are fully vetted and with robust participation from the affected agencies.

Senator WICKER. Do you have an idea of individual officials in China that we could point to as being offenders in this regard?

Mr. PEKOSKE. I do not have that information, sir.

Senator WICKER. All right. Thank you very much, appreciate it, Madam Chair.

The CHAIRMAN. Yes. Senator Klobuchar.

**STATEMENT OF HON. AMY KLOBUCHAR,
U.S. SENATOR FROM MINNESOTA**

Senator KLOBUCHAR. Thank you very much, and thank you, Madam Chair and Ranking Member Wicker, for holding this really important hearing.

I think we all know how bad this is and how scary this is. I was just thinking back to years of classified and unclassified briefings where we were told that this threat, particularly two things, like the power grid, is the biggest threat out there for America, and I know that the Chair talked about the interagency coordination.

I'm just looking at what our biggest challenges to get us to the point where as sophisticated as the people who are messing around with us. I think one of those challenges is workforce and, of course, resources is tied in, but let's say we have the resources. We devote the resources to this. Where do we get the workforce?

Ms. Gordon, in your testimony you highlighted a May 2021 Workforce Assessment Report completed in May by the TSA that showed that the agency lacked qualified personnel with relevant skills.

In your view, how can we increase the number of cyber-security experts in the Federal Government?

Ms. GORDON. Thank you, Senator Klobuchar.

It is an issue not just for the TSA, it's government-wide.

Senator KLOBUCHAR. Right.

Ms. GORDON. Well, we have reported on some potential actions the prior Administrations have taken to address workforce challenges and cybersecurity. They include using the NICE Framework, that's a National Initiative for Cyber Education, to identify and categorize Federal cybersecurity workforce.

DHS has a Cyber Talent Management and that could be expanded. Security clearance process needs to be rationalized and really looked at carefully. It's a very long cumbersome process.

We need to standardize training for cybersecurity for our Federal workforce where it's needed so that the same folks who are out inspecting pipelines and looking at other facilities have the grounding and the same kind of training that we can all rely on.

Cybersecurity Reservist Program has been suggested as an opportunity to create a search capacity, as well.

I would also like to mention the Solarium Commission has mentioned that we could appeal to people who want to provide service to this country, you know, the desperate need we have for the cybersecurity talent, and there could be a consideration to authorizing additional agencies the pay flexibilities that DoD and DHS have for cyber talent.

Senator KLOBUCHAR. Right. Thank you.

Mr. Pekoske, you highlighted the Department of Homeland Security's Cyber Workforce Initiative in your testimony.

Can you talk about some of the challenges, how you think we can get at them? I just think it's a huge deal here.

Mr. PEKOSKE. Yes. Thanks, Senator, and I agree it's a huge deal, and it's called the Cyber Talent Management System that Ms. Gordon referenced.

It's been incredibly successful already. We hired across the department over 300 people in very short order. This allows us to go into a direct hire process which means you don't have to go through the USAJobs process that takes a good amount of time.

Additionally, we have pay flexibilities built into the Cyber Talent Management System and so the cyber talent we brought into TSA, a good portion of those individuals were sourced through this new program.

The other thing that it recognizes is that for cyber talent, you know, some individuals are not necessarily looking at coming into the Federal Government and serving a 20-or-30-year career. Candidly, the Federal Government could benefit from some of those individuals coming into the government, providing value to the government, returning to the private sector, and then potentially coming back.

Senator KLOBUCHAR. Senator Thune and I awhile back put a bill that allowed for this more and, of course, you run into classified issues and things like that, but again we've got to figure that out.

Last question I've got is about I know that Senator Wicker brought up working with the private sector. So, you know, you've got the private sector owning a majority of the critical infrastructure and a recent report highlighted that 51 percent of businesses allocate no resources toward protections against cyber threats. Small businesses comprise about one-half to three-quarters of the victims of ransomware and they can't exactly hire full-time cybersecurity experts.

What do you think the Federal Government should do with the small businesses, with ones that aren't doing enough that are bigger because it's got to be part of the answer? I'm not being negative about these businesses. It's a reality here. How do we work with them better?

Mr. PEKOSKE. Senator, I think a good way to work with small businesses is to provide online available training and discussions on cybersecurity issues and then provide—you know, I mentioned the 200 inspectors that we have across TSA in 47 cities as a resource.

I would much rather prevent a cyber incident than respond to one and so I think the Federal Government and state governments have a role to play in assisting small businesses and providing whatever support.

The other thing that I think is very helpful is running through some exercises just to highlight to businesses where there might be some vulnerabilities that they perhaps had not considered and just figuring out how best to respond to the situations that develop.

Senator KLOBUCHAR. All right. Thank you. I'll ask you something on the record, Ms. Trottenberg. I think I'm out of time here, but

thank you very much and thank you, Madam Chair. I'm going to a Judiciary hearing on nearly the same topic. I somehow think it will not be as pleasant.

The CHAIRMAN. Thank you, Senator Klobuchar.

Senator KLOBUCHAR. All right. Thank you.

The CHAIRMAN. Senator Thune.

**STATEMENT OF HON. JOHN THUNE,
U.S. SENATOR FROM SOUTH DAKOTA**

Senator THUNE. Thank you, Madam Chair.

Welcome, panel. Administrator Pekoske, welcome back to the Committee.

GAO has continued to raise concerns regarding challenges faced by Federal agencies in recruiting and maintaining its cybersecurity workforce. I know that universities across the country have responded to that demand by creating or significantly expanding cybersecurity-related curricula.

For example, Dakota State University in Madison, South Dakota, has significantly expanded its program in recent years and was even designated as a Center for Academic Excellence by both Department of Homeland Security and the National Security Agency.

Could you describe how partnerships between Federal agencies and universities improve TSA's ability to recruit a skilled cybersecurity workforce?

Mr. PEKOSKE. Yes, Senator. Thank you and good to see you.

You know, we have a program in DHS called the DHS Honors Program which is designed to do exactly that. It is to partner with universities, to develop a relationship with them, and then, you know, explore opportunities with graduates of those programs coming into the Federal Government. It's been very successful to date.

The other thing that's important here for us, as well, and Ms. Gordon mentioned this in terms of our ability to assess risk and use all the factors that are needed, particularly in a very changing landscape with respect to surface transportation security in particular, and one of the things that we are looking at very seriously in TSA is developing an academic panel across universities to get the leading edge of risk mitigation thought, risk assessment thought, to ensure that we stay very much with them on that leading edge.

I think we are already there. I just want to have that assessment and really to be able to draw in on that talent.

Senator THUNE. Is TSA currently facing cybersecurity workforce challenges and, if so, what more can you do to improve the recruitment and retention of a cybersecurity workforce, and can you describe actions the agency's currently taking to address some of those workforce shortages?

Mr. PEKOSKE. Senator, we have a Cyber Talent Management System in place across the department at this point. It's a direct hire opportunity, gives us also the opportunity to provide up to 25 percent more pay for a commensurately graded General Schedule position.

This has been very successful for us. We have great hope. This, coupled with the DHS Honors Program and the university out-

reach, we think, will make a very big difference for the department.

Senator THUNE. Ms. Gordon, do you have anything to add regarding cybersecurity workforce challenges and the importance of university partnerships?

Ms. GORDON. I think the cybersecurity challenges that the Federal workforce faces are vast and going to be with us for a long time.

I am not prepared to speak to the linkage between the universities and the Federal workforce needs. Be happy to take questions for the record. Thank you.

Senator THUNE. OK. Ms. Trottenberg, you mention in your testimony the Memorandum of Understanding between DOT and DHS, specifically the updated delineation of responsibilities between PHMSA and TSA for pipeline regulation as required by the TSA Modernization Act of 2018.

Could you describe how these important updates, the MOU, have benefited PHMSA guidance and directives related to pipeline cybersecurity and where you see room for improvement?

Ms. TROTTEMBERG. Yes, thank you for the question, Senator.

I think the updating of that MOU, and I'm sure my colleague will speak about it, as well, gave us the opportunity, I think, to get at, I know, something of interest to this committee, making sure both agencies are bringing information gathered to the table, sharing it with their partners, but we're also making sure we're not duplicating efforts, and I know that's a concern with industry as they're speaking to different government agencies, making sure that they're hearing from us with one voice, that we're not duplicating efforts or working at cross purposes.

So the MOU tries to get at ensuring that our two agencies are in that state of cooperation.

Senator THUNE. OK. Administrator, anything to add on improvements made to interagency coordination on guidance, directives, and inspections by the updated—

Mr. PEKOSKE. Yes, Senator. Just a couple briefly.

One, to add to Deputy Secretary Trottenberg's comment, that MOU is a very significant positive step forward. Built into the MOU is a requirement that we update that at least at 5-year intervals. It was a built-in update mechanism.

The other thing I would add, sir, is the Modernization Act established the Surface Transportation Security Advisory Committee, which includes members from the pipeline sector as well as other surface transportation sector owners and operators, but all of the DOT modal administrations are members of that committee, as is the Department of Energy, CISA, and the Coast Guard.

So that committee, it provides us advice, has a very integrated approach to the advice that they provide us.

Senator THUNE. Could you talk a little bit about—I don't have much time here—quickly improved coordination with PHMSA? Has that enhanced the variety of data resource or data sources, I should say, incorporated into the Pipeline Relative Risk Ranking Tool?

Mr. PEKOSKE. Yes, sir, it does, and it also has a very significant benefit of making sure that whatever security requirements we put in place don't have an unintended safety consequence.

So if we work that up front and then if we find issues, we work that very quickly together, I think it's very positive for everybody. Senator THUNE. Thank you. Thank you, Madam Chair.

The CHAIRMAN. Senator Rosen.

[No response.]

The CHAIRMAN. Senator Rosen.

[No response.]

The CHAIRMAN. If not, Senator Fischer. Senator Fischer, are you available?

**STATEMENT OF HON. DEB FISCHER,
U.S. SENATOR FROM NEBRASKA**

Senator FISCHER. I am, Madam Chairman.

The CHAIRMAN. Thank you.

Senator FISCHER. Thank you very much.

Administrator Pekoske, under the 2020 Annex to the Memorandum of Understanding between TSA and PHMSA, TSA committed "to the extent practicable TSA will consult with PHMSA prior to disseminating requirements, voluntary standards, best practices, and guidelines to the public."

I've heard from some stakeholders that the requirements in TSA's second Pipeline Security Directive issued last week are operationally challenging.

Can you describe the extent of TSA's outreach to PHMSA to seek feedback on the operational impact the Security Directive would have on pipeline operators and to what extent the TSA incorporates PHMSA's feedback into that directive?

Mr. PEKOSKE. Thank you, Senator Fischer, for the question.

We coordinated with PHMSA in advance of issuing the second Security Directive and, to the best of my knowledge, incorporated it as fully as we could PHMSA's input.

Another important thing to consider here is that in the Security Directive, there's a separate paragraph that gives the affected pipeline companies the opportunity to submit alternate procedures and so if they have a way to do something better or if they think there might be a second or third order effect of the Security Directive that we might not have foreseen when we issued the Security Directive, they can come in to us and suggest an alternate way to achieve the same security outcome.

We review those requests relatively quickly and get back to the operators. So there is some flexibility built in to ensure that our intent for security outcomes is achieved without any impacts that might be, you know, for example, an impact on safety that we might not have seen. So there is flexibility built into that process.

Senator FISCHER. With that flexibility, have you seen any concerns, have you heard of any concerns from these companies? Are they taking advantage of that review?

Mr. PEKOSKE. They are, and we have heard of some concerns, and we are willing, ready, and able to take their input with respect to alternative procedures.

The important part of this, too, is that whenever we get input, there's always a discussion as to why we decide to go down a certain path. So I think the pipeline companies will find this process to be one that their input is taken seriously, fully considered, and

they're given a reason why we take the ultimate action we decide to take.

Senator FISCHER. Can you share with us at this point in time, without getting into too much details, some of the concerns that have been expressed to you?

Mr. PEKOSKE. Yes, ma'am. I'll highlight two. One concern is on the very aggressive timelines in the Security Directive and we understand that. We do think that the security issue is immediate and requires immediate action. So, you know, a common concern was, hey, this is a fairly rapid implementation, can we have more time?

The second concern was on have you thought about any safety impacts? The answer is yes, but to the pipeline operators, if you have more information to share with us on that, please do so, and we will fully consider that and we will coordinate that with PHMSA in providing a final reply.

So I think there will be a very good give and take back and forth with the pipeline industry owners and operators and our partner Federal agencies.

Senator FISCHER. You know, as we look at the Security Directive that was issued on May 27th, it required the operators to review their current cybersecurity practices and be able to identify the gaps and also look at remediation measures and to report those results on the review to TSA, to CISA within 30 days and so that would have been the end of June.

The most recent Pipeline Cybersecurity Directive was issued toward the end of July, on the 20th. To what extent did TSA and CISA review the cybersecurity reports that it required from pipeline operators in its May Security Directive and incorporate any of those ideas?

Mr. PEKOSKE. Senator, a couple comments on that. The second Security Directive did consider the input that we'd received from the owners and operators of the first Security Directive.

I'm happy to tell you that we had a hundred percent response from the critical pipeline security operators identified in the first Security Directive. We received the input on the gaps and how they intend to bridge the gaps in the cybersecurity guidelines.

We are still in the process for some of them of reviewing that and certainly if there's an impact on that on the second Security Directive, that's something that we would take into consideration.

Senator FISCHER. You know, obviously we're very, very worried about the risks that we face. So I look forward to hearing from you on some of the information you received and how you're responding to it.

Well, thank you. Thank you, Madam Chairman.

The CHAIRMAN. Thank you, Senator Fischer.

Senator Markey.

**STATEMENT OF HON. EDWARD MARKEY,
U.S. SENATOR FROM MASSACHUSETTS**

Senator MARKEY. Thank you. Thank you, Madam Chair, and thank all of you for being here today.

We had a big explosion, pipeline explosion in Lawrence, Massachusetts a couple years ago. Columbia Gas was the company, and

they had not done a good job at all in upgrading the protections that they were building into their pipeline system and the consequences obviously for ordinary families and businesses in Lawrence and Andover, North Andover were catastrophic.

Much of the lessons that were learned were built into a pipeline safety bill passed through this committee last year and is now the law in the country and I thank the Chairwoman and I'm very proud of the provisions that were included that reflect the lessons that we learned.

Of course, one of the lessons we learned is how much this industry is just way behind the times. That was a company. That was an industry that just hasn't kept up with the times.

So one of my questions is this, I asked the CEO of EMC up in Massachusetts about seven or 8 years ago why don't more companies just upgrade, you know, so they can protect themselves against cybersecurity attacks, and what he said to me was, "well, it's because they just see it as a cost they don't want to assume and they just cross their fingers and hope that they're not going to get hit and if they do get hit because the executives tend to be older, you know, it'll just be on the shoulders of the next generation coming up and they escape it."

So to a certain extent I think the big question for me is the protections are there, you just have to pay for them. Why don't they pay for them? Do you agree with the CEO of EMC who said that to me, that, in general, industry officials just don't want to accept the cybersecurity protection as a cost of doing business in the modern world and they're trying to pretend that it's an older world and that perhaps they as the executives can just escape the responsibility of paying for the upgrades?

Mr. PEKOSKE. Thank you for the question, Senator, and I have a couple comments with regard to that.

First, you're right, a lot of cybersecurity procedures are simple. Cybersecurity hygiene items that have been well laid-out to us as private citizens apply equally to companies. Simple things, such as changing your password or using multifactor authentication on bank accounts and things of that nature.

That's why we relied back on the NIST standards for some of our Security Directive work is, you know, it's an easy standard to go to on the internet. It lays out best practices that industries and people ought to be following.

Senator MARKEY. What happens when they don't want to follow best practices, which they don't? They're there. This is not brain surgery here. Everybody knows that this is a problem and they've known it for 10–15 years. So it's not like the light bulb is going off in these offices. They've already made a conscious decision not to make the investments.

So if they don't adopt best practices, do we need a mandate that they have to adopt best practices?

Mr. PEKOSKE. Well, and that's what the Security Directive does require, sir. It puts a mandate in place for the most critical pipeline systems to do some of those best practices.

I also think that the costs are going up for this. If you look at Colonial Pipeline ransomware \$4.4 million, you know, I often think

about if that \$4.4 million had been invested upfront in their system, what could have been done with that fund.

Senator MARKEY. So a stitch in time saves nine because there's almost an inevitability to a continuation of this and it doesn't necessarily have to come out of Russia or Iran or North Korea. It can come from anywhere, including just somebody in the United States who has malicious intent.

Mr. PEKOSKE. Yes, sir, and in many of the ransomware attacks, sir, are called ransomware as a service. Literally you can buy the service to conduct a ransomware attack against a target. So you don't even have to be sophisticated to do that.

Senator MARKEY. Yes. And it turns out you don't really have to be sophisticated to buy the protections against it either.

Mr. PEKOSKE. That's correct.

Senator MARKEY. You just have to bring in the contractor who will install the protections.

So what is the level of cooperation you're receiving across the country on implementation of those protections?

Mr. PEKOSKE. Sir, the level of cooperation so far has been outstanding. The first Security Directive, we've gotten a hundred percent response. With respect to identifying the gaps against existing cybersecurity guidelines, we have the responses. We're still going back and forth with some of the companies to get additional information to more fully understand.

Additionally, they do now have significant resources on the part of the Federal Government. The Cybersecurity Infrastructure Agency and TSA both have resources to assist, and I think the dialogue with the companies will get even stronger with result of these Directives.

Senator MARKEY. OK. Well, I hope so because obviously consumers pay a big price in increased costs for the energy which they have to pay for because the companies are trying to save money on the short run.

So I thank you, Madam Chair, and I thank all of you for your good work on this issue.

The CHAIRMAN. Senator Blumenthal.

**STATEMENT OF HON. RICHARD BLUMENTHAL,
U.S. SENATOR FROM CONNECTICUT**

Senator BLUMENTHAL. Thank you all for being here and thanks for your great work.

I want to pursue Senator Markey's line of questioning. You know, this idea of spurring more protective measures by the private sector has been an idea here for some time, probably the better part of 5 years, maybe a decade. I remember talking to Senator McCain and Senator Kyle about efforts that could be undertaken and what we encountered was a resistance to taking action and also to reporting.

Have you found that there is more of an inclination to report instances of cyber attacks now than before? Obviously to some extent yes, but are they really reporting as fully as they should be? Let me go down the table.

Mr. PEKOSKE. Senator, yes, they are reporting more than they have in the past. The first Security Directive we issued, the first

thing it requires is reporting for significant incidents because we wanted to get a baseline of information as to what was going on and I think it's also good for the industry partners to see, hey, I'm not alone here. Some of my other companies are experiencing the same thing. We need to get at this. So I expect the reporting to continue to be robust. It will certainly help us.

Senator BLUMENTHAL. Are those reports made public?

Mr. PEKOSKE. No, sir.

Senator BLUMENTHAL. Why not?

Mr. PEKOSKE. The raw data will not be made public but summary data will be made public.

Senator BLUMENTHAL. Why not make the raw data public?

Mr. PEKOSKE. For proprietary reasons for companies they might not want to reveal some vulnerabilities that we have. What we're interested in is we will know that, CISA will know that, and just to provide kind of a baseline across the industry that says, hey, across the pipeline sector, for example, there have been X number of ransomware attacks over the past 30 days and we might highlight in general terms what the nature of those attacks were to provide information we think others need to have to prevent them from happening to those other companies.

Senator BLUMENTHAL. I think one of the reasons there isn't more reporting is that there isn't more reporting. In other words, the public isn't aware of reporting. The companies feel the public isn't aware of reporting. So when there is reporting, it seems like an isolated more embarrassing incident.

If there were more reporting, first of all, the public would become more alarmed as it should be and companies might be more inclined to actually report because they would see it as something that is common and should spur action.

I don't see—I mean, I can understand the proprietary interest, but I don't know how that would prevent more fully reporting the actual dimensions of this threat to our country because, you know, the attackers are aware. Nothing that would keep it from them. They're aware of what they're doing. The companies are aware of it. You're aware of it. The ones who aren't aware of it are the American people. Shouldn't they be better informed?

Mr. PEKOSKE. Yes, sir, I agree they should be better informed, and we do have a responsibility to do that. I was just really referring to the specificity of the attack.

I think providing information that the public can use to be informed as to the scale of what's going on and hopefully over time the trend of having fewer and fewer of these type of incidents will be important.

Senator BLUMENTHAL. Could you send to us, to me information, I assume it's compiled and you can make it available to us in some form, that maybe is nonspecific as to who the company is and then we can follow up as to whether or not the names of the companies could be revealed?

Mr. PEKOSKE. Yes, sir, be happy to work with your staff on providing that information.

Senator BLUMENTHAL. I would appreciate that. And if you had to advise a company as to how to report, what would be your advice?

Mr. PEKOSKE. My advice to a company in terms of reporting cyber incidents would be to report to CISA and we provide in our Security Directive that reporting link so it's very easy to do.

The other thing I think we have a responsibility on the Federal side, whether it's PHMSA, TSA, CISA, or the FBI, when any one of us gets a report to share it with the others because, you know, I don't want to have companies trying to figure out where to report. I want them to report so that we can put it together.

Senator BLUMENTHAL. But would you ever advise a company to try to deal with it on their own without—

Mr. PEKOSKE. I would not, sir.

Senator BLUMENTHAL. OK. Thank you. Thank you, Madam Chair.

The CHAIRMAN. Senator Blackburn, are you ready to go or if not,—OK. Senator Blackburn.

**STATEMENT OF HON. MARSHA BLACKBURN,
U.S. SENATOR FROM TENNESSEE**

Senator BLACKBURN. Yes, indeed. And thank you all. We appreciate your being here and the attention to the issues.

I will have to tell you when I was reading testimony last night, even though it came in late, but reading testimony I feel like there's a little bit of kick the can around on who's responsible for what.

I've talked to some of our pipeline companies in Tennessee and they are very worried about the new requirements in our second Security Directive that you all have put out and, Administrator, this is to you.

They say that the Directive could require them to replace thousands of pieces of equipment all over the country. Not only would it be expensive, take a long time, supply chain shortages are an issue.

So what are the options for the companies when these new Directives are going to be not feasible to achieve?

Mr. PEKOSKE. Senator, if a company feels the new Directive is not feasible, the first thing they should do is contact us so we can have a discussion on why they feel that way and what specifics they have.

Senator BLACKBURN. OK. And so how long would it take for those alternative action plans to be reviewed and accepted?

Mr. PEKOSKE. Sometimes they can be relatively quick, a matter of days. Other times they're more complex, and what we're trying to do is figure out security outcome equivalency. Sometimes that's a little bit more complex to do, but there's a dialogue ongoing as soon as they submit it.

Senator BLACKBURN. So you are looking at this as a directive and not a mandate?

Mr. PEKOSKE. The Directive has mandates in it. The way we look at it is if a company has a different way of doing something that achieves the same security outcome,—

Senator BLACKBURN. So you have flexibility?

Mr. PEKOSKE. They have—they can apply for an alternative procedure and we will review that with them.

Senator BLACKBURN. OK. Let's talk a little bit about the cyber threats and one of the things I hear from companies, whether they're large, mid-size, or small, is inconsistencies in the toolbox that would allow them to move forward. Here's a process, here are tools that are available to you, and it's going to be different.

So you look at a company like Microsoft or Colonial Pipeline or a small business that is doing military contracting in Tennessee. So what tools should they have in the toolbox? What should you be making available to them?

Mr. PEKOSKE. Senator, many of the tools are available commercially to them. What I would suggest is that they look at the standards that we have in the Security Directive and the standards that NIST has set for cybersecurity. It's called the Cybersecurity Framework and they have some publications. That gives the criteria upon which they can measure whether a commercial provider can meet the requirements.

Senator BLACKBURN. So there is a variety of sources and not a one-stop shop?

Mr. PEKOSKE. Correct.

Senator BLACKBURN. OK. Is it a goal of any of you at the table to bring this together in a one-stop shop that would be more helpful to these companies, especially smaller business companies that are doing contracting with some of our critical infrastructure?

Mr. PEKOSKE. Well, Senator, the requirements are not very different. In other words, if there's a requirement for a multifactor authentication of accounts, for example, that's fairly straightforward.

What I was suggesting is there are different sources of assistance that companies can access to meet that standard. So it's not a different varying degree of security. It's the security standard. There are different ways to get to it.

Senator BLACKBURN. Right. The difference, I think, here is that you all know where these items are to be found, these directions are to be found. Many times a business does not and they turn for that guidance and if it is complicated to find the guidance, then compliance becomes not only complicated but costly.

We want to help and do our part in making certain the proper prevention and response mechanisms are there, but it means you all have to not play kick the can but you have to say be more precise in your guidance.

OK. Let me ask you about this. In your testimony, you said this that "TSA has yet to identify or develop data sources relevant to threat vulnerability and consequence of security threats," and GAO made this recommendation to TSA in December 2018, but it had not been implemented as of last month.

So am I correct in understanding that TSA implemented two new Security Directives without all the relevant data?

Mr. PEKOSKE. Senator, the GAO identified 15 recommendations. We concur with all the recommendations. We implemented 12. Three remain outstanding, including the one that you referenced.

Just because a recommendation is outstanding does not mean we haven't done substantial work toward it.

Senator BLACKBURN. But do you have—did you have full and complete data?

Mr. PEKOSKE. We had as full and complete data as we could at the time we issued the Security Directive. We really oftentimes never have full and complete data. That's very hard to achieve. We need to move fast to close a security gap with a system that's vital to U.S. national security and so we used the best data that we had.

But I agree with GAO's recommendation and we are working very hard on that.

Senator BLACKBURN. OK. I know I am out of time. Ms. Gordon, I think you wanted to respond to that.

So, Madam Chairman, I will ask for her response in writing—

The CHAIRMAN. Thank you.

Senator BLACKBURN.—in the interest of time. Thank you.

The CHAIRMAN. Thank you. Thank you, Senator Blackburn.

Senator Capito.

**STATEMENT OF HON. SHELLEY MOORE CAPITO,
U.S. SENATOR FROM WEST VIRGINIA**

Senator CAPITO. Great. Madam Chair, thank you. Thank you for being here.

Not only do I wear a hat in terms of being able to serve on this committee, I also am the Ranking Member on the Appropriations Committee for Homeland Security, which appropriates dollars for CISA. So I know they play a big role here and we talk.

I think in the report there is a lot of talk about collaboration and coordination between TSA and you've already mentioned CISA in your responses.

Are we finding—did we find—I guess this would be for Ms. Gordon—in the examination, have we found that these coordinations are occurring and collaborations are occurring? Are we falling short here? Is there a better way that we can manage that, I think, particularly important aspect of trying to prevent cyber attacks?

Ms. GORDON. Thank you, Senator.

In our work that dates back to 2019, we had a number of recommendations to affirm and encourage PHMSA and TSA to collaborate and coordinate better. To date, they have addressed four of the five recommendations that we had.

The one that remains outstanding is about the Incident Recovery Protocol Plan and more information is needed to fully develop and update, actually update that plan so that it accounts for security risks, threats, changes in Federal law and policy, and TSA has reported back to us that it's working on that and collaborating with PHMSA to do so.

Senator CAPITO. Great. Thank you.

Mr. Administrator, it's good to see you again. Let me ask you this. None of Colonial Pipeline's operational technology was impacted by DarkSide hack. However, there is still a concern that the hackers have obtained information that can still remain a possible impact to Colonial's operation.

Does possession of such information pose a threat to their current operations as you know it or has Colonial worked with TSA to resolve any of these risks and give me the status update on that type of the information that they may still have or may still be out there.

Mr. PEKOSKE. Thank you, Senator. Good to see you, as well, and we work very closely with Colonial as does CISA and the FBI and the Department of Energy.

They brought on private sector and third party companies to help them recover from the ransomware attack and so I know they're working with those companies to assess the extent of the impact, the long-term extent of the impact on their business.

Senator CAPITO. So that's an ongoing investigation?

Mr. PEKOSKE. It is.

Senator CAPITO. It is. I think a lot of the cyber attacks that you hear, both government and private sector, occur very—I don't want to say innocently but the ability to get into the systems occurs by human error. Somebody opens an e-mail, somebody inadvertently, you know, makes it easier to breach the systems.

What's the key to—I guess training is the key to keep—on a preventive measure to make sure that everybody realizes the ramifications of doing that.

Do you have any other perspectives? This would be for the whole panel. Any other perspectives on how to cut down on that human error, a simple mistake can cause a major breach? I don't know who wants to start. Mr. Administrator, why don't you start?

Mr. PEKOSKE. Thank you, Senator. A couple things. One is you're right, training is a key part of it. The other is I just think greater cybersecurity awareness on the part of leadership applies in the government, applies in the private sector, as well.

Long gone are the days when you're a senior official in the private sector or in government where you can say, hey, I don't understand that stuff because it impacts your ability to operate as an agency and your ability to operate as a private sector company.

Some of the requirements in the second Security Directive, which I can't discuss in detail because they are sensitive security information, do provide the information that will allow us to see and the companies to see whether or not they might have some breaches in their IT infrastructure that they ought to take a look at.

Senator CAPITO. OK. Ms. Trottenberg, I think maybe also I may be interested to hear what the Department of Transportation is doing as preventative measures for the things I was talking about.

Ms. TROTTEMBERG. Thank you for the question, Senator, and just to echo the Administrator's comments, I think we see certainly across the transportation sector a lot of the cyber risk is for sort of very basic cyber hygiene issues, that there are obviously some very sophisticated attacks happening at high levels, but a lot of it is fairly basic, and I think TSA Security Directives are hopefully going to really buy down that risk.

You know, as I stated earlier, we are just seeing in the transportation sector obviously as systems grow more sophisticated, the pipeline system, the vehicle systems, that there are more points of vulnerability and I think as the Administrator said, it's no longer just sort of the IT department that has to worry about this. The whole leadership of the organization needs to be involved in cybersecurity.

Senator CAPITO. Right. I mean, if you're looking at vehicles, you know, with all the different sensors going just over a bridge or

something, the ability to disrupt is going to be, I think, I agree, more and more.

Ms. Gordon, did you have anything you wanted to add there?

Ms. GORDON. The Department of Transportation, the Department of Homeland Security serve as the sector risk management agency, lead agency around security for the transportation sector. They have a role to educate, to provide information, to share information about threats to their private sector populations and the private sector owner-operators and that's a vehicle they can use to raise awareness and educate.

Thank you.

Senator CAPITO. Thank you, Madam Chair.

The CHAIRMAN. Thank you, Senator Capito.

Senator Rosen, thank you for being so patient. I think I was supposed to call on you and I missed you when I called on Senator Blumenthal. So I think you're back online and very much appreciate your input.

**STATEMENT OF HON. JACKY ROSEN,
U.S. SENATOR FROM NEVADA**

Senator ROSEN. Thank you. Thank you, Madam Chair.

You know, technology is great when it all works and my microphone wasn't and so we're here today to talk about technology and it's great when it works. It's great when you know how to use it. It's great when you're trained to use it and that you're hyper-vigilant about it as it comes to the area of security, as many of my colleagues, everyone has been discussing the TSA, the Security Directive that was just issued last week, and so I have a few additional questions building on what's already been discussed so far.

So, Mr. Pekoske, does the Directive detail specific safeguards, specific safeguards that pipeline owners and operators should be taking to prevent those ransomware attacks and, if so, can you share those or you can tell me we can take them offline but can you give us a broad perspective of that?

Mr. PEKOSKE. Senator Rosen, thank you and, yes, it does have some very specific requirements that the owners and operators of these most critical pipeline systems need to follow.

I really can't discuss them in great detail in this venue, but I would be most happy to take them offline with you, but very broadly, if you look at the NIST Cybersecurity Framework, it's posted on the NIST website, we reference it in the Security Directive, that will give you an idea of some of the items that we require in the Security Directive.

Senator ROSEN. Thank you. That's great. I'd like to ask this other question building on that.

Does the Directive include penalties for companies that fail to comply and, if not, how can you at TSA ensure that the Directive is effective if there is no way to enforce it?

Mr. PEKOSKE. Senator, there is a penalty, a civil penalty assessed for each incident of noncompliance. The Directive has the force of a regulation and so there are penalties attached for non-compliance.

Senator ROSEN. And I know you probably answered this, but I just want to be sure that the Federal Government, TSA, that you

are, that we are providing guidance to companies to ensure that they're able to quickly implement these mitigation measures, such as the NIST standards and other things as outlined in the report, multifactor authentication.

They're often complex and they take time and so people do need guidance. Are you providing that?

Mr. PEKOSKE. Senator, that's a key part of our mission is, you know, it's very different to require things and not collaborate either before the fact or during implementation. We want to do both and so we collaborated before the fact.

We want to be very good partners with the owners and operators of these pipeline systems because our collective objective is to make them more secure from cyber attacks.

Senator ROSEN. Thank you. I appreciate that.

I want to move on to my Cyber Sense Act because the Colonial Pipeline attack just was a stark reminder that our critical infrastructure is such a target.

So I recently reintroduced the Cyber Sense Act. It's bipartisan legislation that would create a voluntary Cyber Sense Program at the Department of Energy to test the cybersecurity of products and the technologies intended for use in the bulk power system.

This bill would also direct the Secretary of Energy to consider incentives to encourage people to use analysis and testing results when they're designing their products and technologies.

So, Mr. Pekoske and then Ms. Trottenberg, while this program that I'm talking about in my Cyber Sense Act is for energy companies, do you think a similar program for other critical infrastructure, such as pipelines, would be helpful for the pipeline owners and operators and so, Mr. Pekoske, you can begin, please.

Mr. PEKOSKE. Senator, one of the things that we are very carefully looking at is, you know, we put Security Directives out to make cyber measures much stronger on pipeline systems, the most critical pipeline systems, but there are other elements of critical infrastructure and some of these cybersecurity requirements can apply across elements of critical infrastructure. So that's part of the work that we have in front of us is to see what can apply more broadly rather than into a specific sector.

Ms. TROTTEMBERG. I'll just sort of echo the Administrator's comments. Obviously I think what we're seeing with the Security Directives and the pipelines a lot of good work has gone into them, a lot of collaboration with industry across the transportation sectors.

There are clearly other sectors that it's going to logically follow. We've mentioned vehicles today. So I think there will be opportunities, I think, for further collaboration with you all and with TSA.

I think we want to make sure that we're seeing robust cyber protections starting to be instilled in at least all the industries across the transportation sector.

Senator ROSEN. Thank you. I only have a few seconds left. So I'll take this answer off the record, but I would like to have your views on how we invest in cyber personnel and technologies in the workforce pipeline because we can't do any of this work without people trained to do it and so I just want to know your opinions and how we can support companies to invest in developing the personnel

that they need and those resources, and again I see my time's expiring. So I will just take those off the record.

Thank you for your time here today.

The CHAIRMAN. Thank you, Senator Rosen.
Senator Tester, are you ready?

**STATEMENT OF HON. JON TESTER,
U.S. SENATOR FROM MONTANA**

Senator TESTER. Always ready. Thank you, Madam Chair.

I want to thank everybody that's here to testify. This is really an important hearing for critical infrastructure everywhere. I mean, I'll probably focus on the Colonial Pipeline, of course, but the truth is the attack on JBS and all the attacks that I don't know about that have gone on.

So the real question here is when we have critical infrastructure like the Colonial Pipeline, what should be required of that company when it comes to having an attack on critical infrastructure? How broad-based reporting—this is for you, Mr. Pekoske.

How much information should they be required to give to the FBI and CyberCom and all those folks?

Mr. PEKOSKE. Thank you, Senator, and in the first Security Directive we do require that companies report to CISA and CISA will distribute to the other agencies as needed, any significant cyber event and then we define what significant is because—

Senator TESTER. Are there timelines when they have to report it by a certain time?

Mr. PEKOSKE. They do, yes, sir.

Senator TESTER. What is the timeline?

Mr. PEKOSKE. I believe it's 24 hours. So it's very quick.

Senator TESTER. All right. And is it just a report or do they have to do more than that?

Mr. PEKOSKE. Yes, sir, there's detail required in the report and then, of course, you know, depending on what's reported and the severity of the incident, there will always be follow up with CISA and other partners.

Senator TESTER. There's a bill out there, was it 2407, 2407. Are you familiar with that bill? It's a bill on reporting requirements. Is that a yes?

Mr. PEKOSKE. I don't know the contents of the bill, sir, but I will certainly look at it.

Senator TESTER. OK. Are any of you familiar with 2407? No, not so much.

Well, I'd ask that you take a peek at it. It is a bill that delineates out the reporting requirements. Look. I'm all for privacy, but when it comes to critical infrastructure, I think that's called critical for a reason and they need to open their books to make sure that we have the information.

So we know about Colonial. We know that the folks who attacked it have ties to Russia. We also recently learned that China was responsible for an attack on over 20 pipeline operators a decade ago, eight to 10 years ago.

So what additional resources do agencies need to adequately prepare for any possible attack by any foreign actor but particularly when it comes to Russian and China actors?

Mr. PEKOSKE. Sir, additional resources, I think, would be particularly helpful in doing things that kind of raise the baseline of knowledge. For example, resources to support additional training, additional workshops, additional exercises.

There's nothing like a real-world exercise that can be a sobering experience that will cause people to step back and say, OK, there could be some real impacts here, I need to invest more in my own cybersecurity.

The other part, too, if I could briefly, is to embed and we look at this very carefully as does CISA, to try to embed resiliency in some of these systems so that if you are attacked and that may happen,—

Senator TESTER. Yes.

Mr. PEKOSKE.—it may not be preventable, you've got some resilient—

Senator TESTER. So from a TSA perspective, you have everything you need right now to deal with the issue of cyber attacks?

Mr. PEKOSKE. Sir, so we have dedicated a good number of additional resources in cyber. I don't think we're at the point we have everything that we need.

Senator TESTER. So could you do me a favor?

Mr. PEKOSKE. Mm-hmm.

Senator TESTER. If you don't have everything that you need, could you get a list to the Chairman and the Ranking Member and myself of what those extra things are that you might need?

Mr. PEKOSKE. Yes, sir.

Senator TESTER. I'm not saying we're going to do it, but the truth is, is if there are gaps we need to know what those gaps are so that we might be able to address them either through appropriations or through policy.

Mr. PEKOSKE. Yes, sir.

Senator TESTER. Appreciate that. Thank you, Madam Chair.

The CHAIRMAN. Senator Hickenlooper.

STATEMENT OF HON. JOHN HICKENLOOPER, U.S. SENATOR FROM COLORADO

Senator HICKENLOOPER. Thank you all for your time and your service, appreciate it. This is certainly one of the most critical issues facing the country when you look across the entire landscape.

I have a statement here. "A fully prevented cyber attack causes no damage at all." I would argue that's probably mythical. There's no such thing as fully prevent. I guess you count on some occasions but even when you have what some would call perfect defenses, it's a moving target, and I think that backups and recovery plans are achievable if they help mitigate the damage and I think they reduce the pressure for paying ransoms, such as we saw with Colonial.

Administrator, what extent do the TSA pipeline security guidelines include prioritize these resiliency measures, that back side?

Mr. PEKOSKE. Thank you, Senator, and that's really a key critical part of our effort is to make sure that, you know, you can't do everything all at once. You've got to be able to prioritize.

We do this extensively in aviation security. The GAO did a review of our risk prioritization, made some recommendations for us, which we are in the process of implementing, but you hit the nail on the head.

I mean, the idea is to mitigate the risks as much as you can and then understand where you might have some residual risk left, but as I mentioned with Senator Tester, a key part of that whole equation then is to understand what the resiliency is where you have unmitigated risk, as well.

Senator HICKENLOOPER. Got it. And I guess I could ask all of you this. When I was Governor, we spent a lot of time looking at how to value risk management from the point of view of state, local, Federal partners. We created something called the National Cybersecurity Center in Colorado Springs which really focused on providing cybersecurity expertise to local leaders, municipal leaders, county commissioners, state leaders, making sure they have education outreach up and down the chain of command within states.

Why don't we start with you, Administrator? How do you believe that TSA can improve the coordination and information-sharing that's necessary up and down—from state to state but also especially vertically within states?

Mr. PEKOSKE. Sir, and that's one of those topics where you can make a number of improvements and you can also say at the very same time much more work needs to be done, and I applaud the initiative of having cybersecurity centers that are spread throughout the country and one of the things I think is really important about those centers, you mentioned the ability to train leaders and I think particularly when it comes to committing investment to close cybersecurity gaps, it needs to be the leaders of private sector companies and leaders of public agencies and organizations that kind of understand when somebody comes to them and says, hey, I need to get this amount of resources to close this gap, understands why that's so important.

Senator HICKENLOOPER. Right. Either of you other want to take a shot at it, a swing?

Ms. TROTTEBERG. I'll just add a couple things, Senator. First of all, I think, you know, one thing in what I hope is the deepening relationship between DOT and TSA, I think one of the useful things we bring to the table, as you know well, is on the transportation side very close relationships with state, local government transportation agencies, and I think we're trying to increasingly, you know, again within our authorities and our capabilities, help them think through some of the cyber issues they're facing and work closely with TSA on that front.

Just to go back to your original question on sort of mitigations, I think one of the interesting lessons of Colonial Pipeline is PHMSA stood up and helped Colonial Pipeline do manual operations, something that they had not done for many, many, many years, and now one thing we're going to be looking at going forward with pipeline operators, can you get up and running manually should an incident occur, so we can be sure we don't have those disruptions.

Ms. GORDON. As GAO has reported on the cybersecurity needs for the Federal Government, there is a need for a comprehensive Federal cyber strategy with the appointment and approval of a national cyber director. This is a focused person in a role and responsibility and now there's a need to update the Federal cybersecurity strategy.

I think when that is updated, then the sector risk management agencies can help in coordinating down to the state, territorial, tribal, local levels.

Senator HICKENLOOPER. And do we think that that's going to get us to another mythic proportion, that single point of contact with the Federal Government? I know that's been an issue for many Governors and hence probably Senators, as well. I mean, where do you connect with the Federal Government on these issues?

Ms. GORDON. The sector risk management agencies for each sector.

Senator HICKENLOOPER. About how many of those?

Ms. GORDON. There are nine.

Senator HICKENLOOPER. Nine. I stand corrected. All right.

Ms. GORDON. CISA's always the place to go for cybersecurity information, of course.

Senator HICKENLOOPER. Got it. All right. Thanks. I'll yield my time back to the Chair. Thank you.

The CHAIRMAN. Senator Scott, are you ready? Senator Scott and then Senator Warnock.

**STATEMENT OF HON. RICK SCOTT,
U.S. SENATOR FROM FLORIDA**

Senator SCOTT. Thank you, Chair.

Thank each of you for being here. Thank you for your service.

Do we all agree that the actions—if you look at the actions of Communist China, they're becoming increasingly dangerous and a bigger threat possibly to American cyber-security. I think we all agree with that, right?

[Witnesses nodding their heads.]

Senator SCOTT. Anybody think they're going to get any better? So what can we do to get government, especially the Federal Government, and the private sector to start working together better to make sure that we don't have these ransomwares and we have worse attacks going forward? What would you all—what's your suggestion?

Mr. PEKOSKE. Senator, I think one of the key things is to—this is a partnership. The government cannot protect alone private sector-owned infrastructure that might be subject to attack from a nation state and so I think the increased level of coordination and co-operation and partnership between the government and the private sector is really important.

We have always done that in the aviation side and we do it now, now that we've regulated, surface transportation security in terms of two Security Directives. That give and take and that back and forth is very important for our mutual success.

Senator SCOTT. Any other suggestions?

Ms. TROTTERBERG. I think I'll just add to what the Administrator said. The aviation is a good model where obviously there has been

a very close nexus between FAA, TSA, and the private industry. It's starting to develop now in pipelines to a greater degree obviously driven in part by the Colonial Pipeline cyber attack, and I think you'll see that will continue to grow across other sectors.

I think we're finding a good template of bringing private industry in, working collaboratively. I think as the Administrator says, neither side can do it all on its own. Both sides are going to have to bring their resources to the table.

Senator SCOTT. Yes. Good.

Ms. GORDON. There are a number of models in how we work with the private sector and the Federal Government. In critical infrastructure, there's the CFAS Program which is a little more of a regulatory model but it uses performance standards in order to bring private sector into meeting specific standards but allowing them to do it the way that they feel best meets those standards. They just are measured against meeting standards. It's also a risk-based approach.

There's a different regulatory model in the energy sector and we see a change here with the May and July Security Directives that TSA has put out moving from a voluntary partnership model to a little more of a regulatory stance in the transportation sector.

Senator SCOTT. Do you think we need to have—the private sector needs to disclose to the proper Federal agency when they have an attack, and do you believe it ought to just be to the Federal agency? Do you think it ought to be to the public? Do you think there ought to be more disclosure about, you know, if they're paying ransomware, things like that?

Mr. PEKOSKE. Senator, the first Security Directive we issued at the end of May requires exactly that reporting. It's reporting of all significant cyber incidents and we define significant. So we're not looking at some very minor issues that are going on every single day in every company but really the most significant ones, and then from our perspective, it's important for us to share generally that information so that the American public kind of understands the baseline of cyber activity.

Senator SCOTT. Do all of you agree on disclosure or what's your thought process? Do you think it ought to be to the public or just to a Federal agency?

Mr. PEKOSKE. So the reporting is to the Federal agencies and there will oftentimes be company proprietary information in that reporting, necessarily so, so that the Federal agencies that are trying to assist fully understand the scale and the scope of the attack.

I think the Federal agencies have a responsibility to anonymize that data and provide it in general format to the public.

Senator SCOTT. So are there best practices that we ought to be—whether it's dictating, but best practices that we ought to be telling the states and local governments what they ought to be doing?

Mr. PEKOSKE. Yes, sir, and a number of those best practices are embedded in the Security Directives, but for the states that don't have the Security Directive, I would refer to the NIST standards, the NIST Cybersecurity Framework, which is excellent.

Senator SCOTT. OK. Thank you, Chair.

The CHAIRMAN. Thank you, Senator Scott.

Senator Warnock.

**STATEMENT OF HON. RAPHAEL WARNOCK,
U.S. SENATOR FROM GEORGIA**

Senator WARNOCK. Thank you, Madam Chair, for hosing this conversation on Pipeline Security: Protecting Critical Infrastructure.

Obviously this is an issue that all of us are concerned about. We've been able to see really just a glimpse of the potential consequences. I say that as someone who hails from the state of Georgia. Colonial Pipeline, of course, runs directly through my state.

Following the ransomware attack on Colonial, over 40 percent of the gas stations in Georgia were out of gas. At the height of the situation, over 70 percent of the stations in the Atlanta area were without gas. This attack caused a lot of turmoil to put it lightly in Georgia and across the country.

Folks couldn't go to work, small businesses suffered, families in Georgia who were already barely getting by had to deal with another crisis after a challenging year. Ransomware attack on the Colonial Pipeline had very real consequences for working families across Georgia and exposed obviously national security concerns, dangerous vulnerability in our critical infrastructure.

Administrator Pekoske and Deputy Secretary Trottenberg, my first question is simple. What specific steps are your agencies taking right now to prevent a cyber attack like this from happening again? Administrator Pekoske?

Mr. PEKOSKE. Thank you, Senator. We've taken two very specific steps recently.

We issued two Security Directives which basically are regulations that are implemented in an emergency to require action on the part of private sector entities. The first Security Directive required reporting, required the establishment of a cybersecurity coordinator that was available 24/7, and also required private sector pipeline companies to assess their cybersecurity against the cybersecurity guidelines that we had published in coordination with them for many years.

The second Security Directive has specific actions to ensure that the companies increase their overall cyber-security. Those specific actions are sensitive security information, so they're not public, but the whole idea behind the second Security Directive is to make sure that, in addition to the reporting and the coordinator and the gap analysis, that we take specific actions to prevent an attack from occurring.

Additionally, the second Directive requires something called the Architecture Design Review and the purpose of these architecture design reviews is to take a look at the IT architecture of a company and determine whether or not a business IT system might bridge into an operating technology system which could in the case of a pipeline affect the flow of product through that pipeline and so we want to just make sure that there is good separation between those two systems.

Additionally, we have a requirement in the second Security Directive for some contingency planning on the part of pipeline companies. When I say pipeline companies, these are the pipeline companies that are the most critical, not all pipeline companies, and

the ones that account for about 85 percent of the product that flows in the country.

Senator WARNOCK. Deputy Secretary Trottenberg.

Ms. TROTTEMBERG. Yes, thank you, Senator. DOT through PHMSA is regularly inspecting and regulating pipeline operations around the country. We're inspecting the physical integrity of the pipelines. We're in control rooms and so we are looking for where we see security issues and working closely with TSA and CISA on that and I think one lesson I was mentioning to Senator Hickenlooper, as a mitigation plan, we're also making sure, as Colonial had to do quickly, in the case of the cyber attack, can you manually operate your system so that you don't see the kind of disruptions that you saw on the ground in Georgia and other states if there is some kind of an attack.

We're wanting to make sure that now operators have those mitigation plans in place and, as always, other parts of our agency, particularly Federal Motor Carriers and MARAD, are working with local governments and state governments on the ground if there are cases where we see issues with fuel deliveries and shortages, making sure we can get trucks and ships delivery.

Senator WARNOCK. Thank you. As we focus on preventing future major cyber attacks, I think that some of the work that's happening in the state of Georgia can be helpful in these efforts.

I'm particularly proud that our colleges and universities, like Augusta University and Columbus State University, have made the forward-thinking decision to invest in cyber education.

Ms. Gordon, why is increasing the STEM and cyber education of our young people critical to addressing gaps over the long term and cybersecurity expertise in the TSA workforce, including TSA employees who perform cyber-security inspections?

Ms. GORDON. Senator, there is a great need to increase the cybersecurity workforce, not just in the TSA but in other areas of the Federal Government, and the pipeline of educated, dedicated individuals who are willing to work in the Federal Service and apply their cyber-security knowledge base is greatly needed.

Senator WARNOCK. Thank you all so much for those responses and I look forward to working with my colleagues on this committee and here in the Senate to make sure that we have the kind of cybersecurity resilience necessary for this moment.

Thank you, Madam Chair.

The CHAIRMAN. Thank you, Senator Warnock.

Senator Luján, are you available?

[No response.]

The CHAIRMAN. Senator Peters.

[No response.]

The CHAIRMAN. We have a vote ongoing and so I'm not sure how much we're going to be able to fit in but while we're looking to see if there are any other members who want to participate, I wanted to—Senator Blackburn had brought up this question which was to you, Acting Director Gordon, about in your testimony you state that "TSA has yet to identify or develop data sources relevant to threat vulnerability and consequences." I think that was a quote she was reading.

GAO had made this recommendation to TSA in December 2018, but it had not been implemented as of last month. Am I correct in understanding that TSA implemented two new Security Directives without the relevant information about possible threats to the pipelines in the USA?

Ms. GORDON. I would like to clarify our open recommendation. It isn't that the TSA doesn't have information on threat vulnerabilities and consequences. It's that our recommendation is that they seek beyond just the information they collect from owner-operators to other data sources and bring in things like the information that PHMSA has about pipeline physical conditions as well as prior cybersecurity attacks and the like. So bringing in additional data sources to account for when they are prioritizing and using the relevant ranking tool to inspect a pipeline.

The CHAIRMAN. Any other witnesses want to comment on that?

Mr. PEKOSKE. Senator, I agree with Director Gordon's comment. You know, we are very cognizant of the threats. It's making sure that we import, as she said, as much additional data as we possibly can, but I'm very confident in the pipeline companies that we covered under our Security Directive that we do have the most critical companies within that list and, you know, I think we'll continue to improve our risk assessment/risk management tool, but clearly we're very clear about the threat that we face.

The CHAIRMAN. I think, Ms. Gordon, though, is saying that—she's saying that you could be more—there's nothing to the recommendations that you had to be limited.

Look. I think this has been greatly illuminating in so many different ways. Again, we appreciate everybody being here, but I think these are asymmetrical threats and let's face it. You represent bureaucracies and as much as I want to see people coordinate, the issue is you got to flatten the bureaucracy. You got to flatten the bureaucracy and you got to get a game plan and you got to implement new technology and you got to get it done fast and so I would hope that we would all take heed of the incident that happened and say what is that now that gives us that ability to act in a more robust way than we're acting?

So everybody's competent here. Everybody's working hard. Everybody, but something big has changed, OK, in that these threats are very, very asymmetrical and it's not an advantage that we're hierarchical. It's not an advantage.

So we've got to get out of these little silos that, you know, are cozy for us and get the information and data and push our colleagues and push the windows out of this bureaucracy approach and get something implemented that is going to help us all.

So I think the data is there and again I appreciate my colleagues in FERC making, you know, their efforts known in this.

So I hope maybe we could have another hearing on this in the very near future on exploring some of those technology solutions that we should be implementing and how we can get them implemented faster because I really think that's where we are. I think that this is, you know, going to continue to be one of the biggest challenges that we face just because we live in an information age and the threat by state actors as well as people who just want to make money off of this are going to continue and I think, you

know, with a little more, you know, discussion, breaking down these silos, I think we can get to some solutions and get them implemented faster.

So thank you all very much for being here. The hearing record will remain open for one week and any Senators that would like to submit questions for the record should do so within that one week.

And this concludes our hearing today. Thank you.

[Whereupon, at 11:48 a.m., the hearing was concluded.]

A P P E N D I X

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO
HON. DAVID P. PEKOSKE

Colonial Pipeline Attack. In TSA's first Security Directive issued in May, you required critical pipeline owners and operators to identify any gaps and related remediation measures to address cyber-related risks in their system and report the results to TSA within 30 days.

Question 1. What were the results of that report, and were there common themes identified across critical pipelines that were similar to the Colonial Pipeline attack?

Answer. As required under the Security Directive, pipeline owner/operators were required to conduct a vulnerability assessment on their Information and Operational Technology systems and identify any gaps. Generally, based on the self-assessment responses provided by applicable owner/operators, the common gaps noted including needed improvements to pipeline operator security plans, configuration management, incident response, continuity of operations, and participation in cybersecurity response and recovery exercises.

Question 2. Prior to this attack were there any concerns raised about potential cyber vulnerabilities for Colonial Pipeline?

Answer. TSA has conducted Corporate Security Reviews (CSRs) and Critical Facility Inspections/Critical Facility Security Reviews (CFSRs) with Colonial Pipeline. The results of these reviews are protected from disclosure as Sensitive Security Information.

TSA Security Directive #2. On July 20, 2021, TSA issued a Security Directive that required the 100 most critical pipeline owners and operators to take specific action to enhance the cybersecurity of critical pipelines. However, in the natural gas industry there are 1,344 distribution pipeline operators, 165 transmission pipeline operators, and 382 natural gas gathering line operators. In the hazardous liquid space there are 550 pipeline operators and 25 liquid natural gas facility operators.

Question 3. What steps is TSA taking to ensure the rest of our pipeline systems are secure beyond just the top 100 owners and operators?

Answer. Although TSA's risk-based focus has been on the most critical pipeline owners and operators, TSA will continue to provide relevant security information and guidance to all pipeline owner and operators. TSA provides specific voluntary guidance to all pipeline owner and operators as outlined in the TSA Pipeline Security Guidelines (Guidelines). The Guidelines were updated in 2018 with a specific focus on cybersecurity measures and again in 2021 (Change 1) regarding the criteria to identify critical pipeline facilities. TSA expects to update the Guidelines again in calendar year 2022 after consultation with industry. This update will focus on additional cybersecurity measures included in the Security Directives, as well as updated guidance based on feedback received from the pipeline industry.

While section 1557 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110-53; August 3, 2007) required TSA to focus its assessments on the 100 most critical pipeline operators, the Guidelines are applicable to all operational natural gas and hazardous liquid transmission pipeline systems, natural gas distribution pipeline systems, and liquefied natural gas facility owner/operators. TSA conveys the importance of the Guidelines, provides security alerts, and distributes sector-wide security information to the larger stakeholder population with monthly pipeline industry calls and information sharing via e-mail distributions to designated cybersecurity coordinators and pipeline security managers.

Question 4. How does TSA plan on ensuring compliance with the directive? What enforcement actions can TSA take against uncooperative operators?

Answer. TSA will assign trained, credentialed Transportation Security Inspectors to conduct inspections of regulated parties under the Security Directive. TSA will use its inspection authority in accordance with 49 USC 114(f) to verify that the covered pipeline owner/operators are complying with the provisions of its security direc-

tives. TSA will use its progressive enforcement process that can result in civil penalties being levied against non-compliant parties. TSA will ensure compliance with each applicable mitigation measure through scheduled on-site visits and requests for documentation to perform verification of compliance of mitigation measures. Both verification processes are consistent with TSA's compliance inspection methodology.

TSA will follow the regulatory framework for TSA's enforcement and investigative procedures found within 49 CFR part 1503. TSA's enforcement process includes the Action Plan Program, a program which provides the opportunity for eligible parties and TSA to first discuss and reach an agreement on corrective actions to address the root cause of any security vulnerability or noncompliance with TSA's security requirements which qualifies for this program, and then resolve that vulnerability or noncompliance with administrative action instead of a civil enforcement action.

If an alleged violation is discovered and it is not addressed through on-the-spot counseling or resolved through an action plan, TSA will send the owner/operator a Letter of Investigation notifying them of the date, time, and a summary of the alleged violation. The owner/operator will be given the opportunity to respond in 30 days and TSA will consider the owner/operator's Letter of Response (LOR) to the violation. After receiving the LOR or after the specified period of time has elapsed, TSA will either close the matter with no action, close the matter with an administrative action, or recommend a monetary civil penalty.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. KYRSTEN SINEMA TO
HON. DAVID P. PEKOSKE

Pipeline Security Initiative. In your testimony, you mentioned that the Pipeline Cybersecurity Initiative (PCI), launched in 2018, aims to assist pipeline owners and operators to prepare for and respond to significant cyber events.

Question 1. Aside from the May and July 2021 pipeline security directives issued by the Transportation Security Administration (TSA), what other actions are needed to ensure that the Cybersecurity and Infrastructure Security Agency (CISA) and TSA can make the PCI more effective in helping pipeline companies identify cybersecurity risks and develop strategies to prepare for, respond to, and mitigate significant cyber events?

Answer. TSA has a close and collaborative partnership with the Cybersecurity and Infrastructure Security Agency (CISA), U.S. Department of Transportation (DOT), and the U.S. Department of Energy (DOE), including technical support from the DOE National Laboratories. The Pipeline Cybersecurity Initiative (PCI) brings together the expertise of multiple interagency partners to conduct a series of activities to assist pipeline owners and operators to enhance their cybersecurity posture. Most recently PCI, TSA, and CISA's Cybersecurity Division Insights Team conducted a review and analysis of the first pipeline Security Directive and prepared a summary of findings. The results of this analysis are being used to identify notable trends and gaps in the cyber preparedness across the most critical pipeline owner/operators and to produce a summary of corrective actions highlighting appropriate recommendations and mitigations.

Throughout Fiscal Year (FY) 2021, TSA and CISA collaborated on Validated Architecture Design Reviews (VADR), associated analysis, and ultimately limited results-sharing with industry. Through PCI and other similar Pipeline-focused initiatives, TSA will continue to collaborate with interagency partners and pipeline owners/operators to prepare and respond to significant cyber events.

Other actions are needed to ensure that CISA and TSA can make the PCI more effective in helping pipeline companies identify cybersecurity risks and develop strategies to prepare for, respond to, and mitigate significant cyber events. These actions include:

1. Ensuring that the results from architecture reviews completed by third-party assessors (*i.e.*, those not done by CISA and Idaho National Labs) as required by SD-2 are made available to TSA and CISA and that the findings are captured in a way that can be compared with existing VADR data that was collected in FY 2021.
2. Pipeline companies should take advantage of tools and resources offered by CISA, such as cyber hygiene scanning, phishing campaign assessments, and penetration testing so that CISA can build a more holistic view of pipeline operators' overall cybersecurity, as opposed to only control systems.
3. Findings from aggregated assessments of pipeline data should be mapped back to industry standards (*e.g.*, API 1164, IEC 62443) to better communicate infor-

mation in the language that the pipeline industry and its associated stakeholders (e.g., manufacturers and integrators) utilize.

4. API 1164, once completed, could be included as an element of the CyberSecurity Evaluation Tool (CSET) self-assessment. Efforts are further coordinated through the Oil and Natural Gas Subsector Coordinating Council, which is co-chaired by DOE and DHS, with representatives from TSA and DOT, as well as other Federal agencies as appropriate.

Challenges to Implementing Pipeline Security Directives. The Senate Commerce, Science and Transportation Committee hearing spent some time discussing the challenges of obtaining qualified cyber security experts for TSA as well as the rest of the Federal government and private industry.

Question 2. Aside from this talent gap, what other key challenges does TSA face in implementing the new pipeline security directives and in better positioning the agency to prepare for, respond to, and mitigate future significant cyber events to its own systems?

Answer. A key challenge that TSA faces is ensuring that there is a mutual understanding of the lexicon of Security Directive # 2 definitions and nomenclature. As Security Directives are new to the pipeline mode, TSA must ensure owner/operators understand the tools available to them to work with TSA towards compliance with the Security Directive. These include alternative measures requests and requests for additional time through the TSA Action Plan process. Additionally, TSA is mindful of owner/operators impacted by acts of nature and is allowing those affected by hurricanes and wild fires additional time to complete required actions. Another key challenge is the continued evolving nature of the cybersecurity threat. As pipeline transportation systems build in automation and digitalization operational technology systems that converge with Information Technology (IT) networks for efficiencies and remote operations, the threat to their networks' cybersecurity grows. Another challenge TSA faces is to ensure pipeline owner/operators providing TSA with SD required information, take the appropriate measures to protect that data while in transit (such as encryption, HSIN, or TSA Secure Portal).

Regarding TSA's preparation, response, and mitigation measures for any future significant cyber events against its own systems, we hold each TSA system owner of a system that connects to a TSA system responsible to the same cybersecurity standards and governance as directed by the Federal Information Security Management Act of 2014, Pub. L. 113-283, (Dec. 18, 2014), as amended, Office of Management and Budget, National Institute of Standards and Technology, and the U.S. Department of Homeland Security (DHS). Before granting approval for TSA IT systems connectivity and operations, all system cybersecurity risks must be identified and understood prior to acceptance of any risk or non-compliance with mitigations is approved and authorized by the TSA authorizing official.

Pipeline Cybersecurity and TSA Directives. TSA's May 2021 pipeline security directive mandated that a pipeline owner/operator have a cybersecurity coordinator, who (amongst other things) is required to report significant cybersecurity incidents to CISA.

Question 3. Does this or the July 2021 security directive have any provisions that would require a pipeline owner or operator to report ransomware payments paid out in response to cyberattacks? If no, do you feel like this should be required of pipeline companies and what parameters would need to be provided?

Answer. TSA Security Directive Pipeline-2021-01 requires the reporting of cybersecurity incidents to CISA. It does not require the reporting of a ransomware payment paid out in response to a cyberattack. While the reporting of ransomware payments is not particularly relevant data to TSA's mission for the prevention of and preparation for cyberattacks, it could be of value for law enforcement and other investigative purposes. Information as to whether or not a payment had been made by a victim of ransomware would normally be a part of the investigative follow-up.

Question 4. If TSA receives notice of a cyberattack or a ransomware payment from a pipeline owner or operator, what is your understanding of the interagency process for coordinating efforts amongst key Federal agencies? If TSA is notified rather than CISA, would that serve to meet the new incident reporting requirements as prescribed in the May security directive, and would TSA officers know how to start the interagency coordination process amongst key stakeholders to quickly gather information and respond to the attacks?

Answer. Overall, the U.S. Government works toward ensuring that a notification to DHS, the Federal Bureau of Investigation, or a Sector Risk Management Agency, is a notice to all, regardless of which agency is notified first. If TSA receives a notice of a cyberattack or ransomware payment from a pipeline owner or operator, TSA

would notify other relevant Federal agencies such as CISA, DOE, and their coordination efforts amongst the Federal agencies would be guided by Presidential Policy Directive 41 (PPD-41).

Pipeline Security Directive 2021-01 requires identified pipeline owner/operators to contact CISA to report any cybersecurity-related incident. If a pipeline owner/operator notified TSA rather than CISA, TSA would immediately notify CISA. TSA's Transportation Security Operations Center routinely coordinates incident response with CISA. Additionally, DHS incident reporting guidelines would require the reporting of certain incidents to the DHS National Operations Center, which would assist with additional incident response coordination.

Question 5. With the May and July pipeline security directives, TSA has moved into the role of a regulator of pipeline companies. How will this impact TSA's work in building and maintaining robust public-private partnerships with pipeline owners and operators to ensure the safety and security of this critical infrastructure? What steps are you taking to work to maintain trust and ongoing cooperation with your key private sector stakeholders?

Answer. TSA recognizes that by issuing these Security Directives, which may subject covered owner/operators to civil enforcement action, some aspects of its engagement with pipeline owners and operators may change. However, TSA has a strong history of collaborative engagement with its stakeholders and will continue this relationship through information sharing, identifying mutual security objectives, and collaboration to reduce risks and enhance resiliency.

TSA is working directly with pipeline owners and operators to achieve compliance with these Security Directives and enhance their cybersecurity posture. TSA also continues to partner with industry on its long-standing, well-established voluntary programs such as the CSR and CFSR, and the most recent PCI-led VADR efforts. As important pipeline security programs and initiatives are identified or developed, or information sharing and threat briefing opportunities arise, TSA will continue with its history of collaboration with the Surface Transportation Security Advisory Council, the Pipeline Subsector Coordinating Council, the Oil and Natural Gas Subsector Coordinating Council, industry trade associations, and direct engagement with pipeline stakeholders. TSA is committed to maintaining its successful public-private partnership with pipeline owners and operators to ensure that the necessary security measures are in place while maintaining operational safety and efficiency.

Question 6. It is noted that the May and July pipeline security directives, these apply to the major owners and operators of TSA-designated critical pipelines. Are there any plans to have similar requirements or guidance issued for the smaller pipeline owners?

Answer. TSA uses a risk-based approach to identify critical pipeline owner/operators that are subject to Security Directives. The method used considers multiple variables to assess threat, vulnerability, and consequence. Data sources include, but are not limited to, publicly available throughput volumes, and information from the U.S. Departments of Defense, Transportation, and Energy. Volumetric throughput is given the most weight. Although there are no current plans to subject non-critical pipeline owner/operators to TSA Pipeline Security Directives, TSA may reconsider this position under the appropriate circumstances. TSA provides specific voluntary guidance to all pipeline owner/operators in the TSA Pipeline Security Guidelines (Guidelines). The Guidelines were updated in 2018 with a specific focus on cybersecurity measures and again in 2021 (Change 1) regarding the criteria to identify critical pipeline facilities. TSA expects to update the Guidelines again in calendar year 2022 in consultation with key industry stakeholders. This update will focus on additional cybersecurity measures included in the Security Directives as well as updated guidance from the pipeline industry *e.g.*, the recently updated cybersecurity guidelines from the American Petroleum Institute (API 1164).

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BEN RAY LUJÁN TO
HON. DAVID P. PEKOSKE

DOE Role in Pipeline Security. Securing our oil and natural gas pipeline systems is a hard problem, one that needs research, just like other critical infrastructure. Several national laboratories support the DOE's cyber office and DHS' Cybersecurity and Infrastructure Security Agency (CISA) both in understanding cyber vulnerabilities for energy technologies and in modeling the resilience and reliability of these systems.

Question 1. How is TSA working with the Department of Energy and its National Laboratories to access their cybersecurity subject matter expertise?

Answer. In TSA's pipeline coordination role as the co-Sector Risk Management Agency for the Transportation Systems Sector, TSA continues to take a whole-of-government approach to strengthening the physical and cybersecurity of pipelines with multiple government agencies. We work in collaboration with CISA and the DOE's Office of Cybersecurity, Energy Security, and Emergency Response, as Sector Risk Management Agency to the energy sector, DOE's Idaho National Laboratory (INL), and the DOT's Pipeline and Hazardous Materials Safety Administration. Interagency agreements have allowed for TSA to utilize INL expertise to provide extensive cybersecurity training for our cyber Pipeline Security Assessment Team (PSAT). The cyber PSAT staff have received a wide variety of introductory and continuing cybersecurity education opportunities including at the INL training facility in Idaho Falls, ID.

Question 2. Does TSA currently face barriers that prevent it from more coordination with DOE and the National Laboratories to improve resiliency of pipeline cybersecurity?

Answer. TSA relies on the availability of Congressional funding to integrate advanced cybersecurity tools and other technical capabilities offered through INL, which in turn supports newer and more intuitive ways to improve pipeline cybersecurity and resiliency. Low or a decrease in funding may hinder or prevent more coordination with INL in the ability to support contractual interagency agreements.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARSHA BLACKBURN TO
HON. DAVID P. PEKOSKE

Background: During the hearing, you talked about GAO's recommendations to TSA. Specifically, the recommendation for TSA to seek more comprehensive data information from sources beyond just pipeline operators to contribute to better assessing the cyber threat environment.

Question 1. Why would TSA move forward with directives to the pipeline industry without full and complete data?

Answer. The decision to issue Security Directives 2021-01 and 2021-02 was based on a determination that immediate action was necessary to protect transportation security. This determination reflected information regarding the current risk as well as threat information from classified, unclassified, and open source material. It is important to note that the Government Accountability Office's (GAO) recommendation related to seeking more comprehensive data from sources beyond pipeline operators that could inform the Transportation Security Administration (TSA) Pipeline Risk Ranking Tool, resulting in a more holistic view of risks to pipeline systems; it was not focused on assessing cybersecurity threats.

Question 2. What is your plan for collecting the sources of outside data GAO has identified?

Answer. TSA continues to work on the GAO's recommendation. The Agency is collecting information from multiple sources, including the U.S. Department of Transportation's Pipeline and Hazardous Materials Safety Administration (PHMSA), the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), the Department of Energy, and the Federal Energy Regulatory Commission, as well as the industry-led Pipeline Subsector Coordinating Council and Oil and Natural Gas Subsector Coordinating Council. These efforts are intended to ensure that TSA is aware of and considering all risks to the pipeline sector. In particular, TSA discusses risk elements with both Federal and industry partners in conjunction with the CISA Pipeline Cybersecurity Initiative, which meets regularly. TSA directly engages with approximately 200 industry security personnel on current security risks and initiatives during regular TSA-led stakeholder meetings.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO
HON. POLLY TROTTEMBERG

PHMSA Control Room Management Reviews and Audits. The Pipeline and Hazardous Materials Safety Administration (PHMSA) conducts routine audits and reviews of pipeline operators' control room management and other elements of pipeline operations.

Question 1. As a part of these reviews and audits, does PHMSA consider cybersecurity hygiene? If so, what elements of cyber security does PHMSA evaluate as part of these reviews and audits?

Answer. As part of a five-year program started in 2019 to promote good cyber hygiene with pipeline operators, PHMSA offers cybersecurity risk discussions to pipeline operators when it conducts regulatory inspections of Control Room Management (CRM) programs. PHMSA's intent is to raise awareness throughout the entire pipeline industry of cyber vulnerabilities and assure companies know about the Transportation Security Administration's (TSA) cybersecurity measures, as detailed in TSA's Pipeline Security Guidelines (current version April 2021). Further, because cybersecurity issues can affect pipeline's physical operations, PHMSA invites pipeline operators to discuss cybersecurity issues. The cybersecurity risk discussion is not part of PHMSA's CRM compliance inspection, nor does it function as an inspection. Its purpose is to raise awareness of the importance of thorough cybersecurity practices—and to better prepare both regulators and operators for cybersecurity incidents.

PHMSA advises pipeline operators that the TSA is the regulatory authority for security issues. PHMSA documents if an operator agrees to engage in a cybersecurity risk discussion but does not record the details from the cybersecurity risk discussions. If the discussions result in the identification of significant cybersecurity risk or vulnerability, PHMSA shares those findings with TSA and the Cybersecurity and Infrastructure Security Agency (CISA). As part of the five-year program, PHMSA has offered to have discussions with 113 pipeline operators. Approximately 50 percent have declined. PHMSA will offer to conduct cybersecurity risk discussions for the remaining 153 operators within the next three years. Since the May 2021 cybersecurity incident involving Colonial Pipeline, 100 percent of operators have accepted PHMSA's invitation to participate in a cybersecurity related discussion during CRM inspections.

Question 2. Does PHMSA alert the Transportation Security Administration (TSA) about if they identify any cybersecurity concerns or vulnerabilities identified as a part of PHMSA's oversight of pipeline operators?

Answer. Yes, PHMSA provides any significant cybersecurity risks or vulnerabilities identified during a cybersecurity risk discussion to TSA via secure file transfer or by password protecting a word document and marking it Sensitive Security Information (SSI).

NIST Cybersecurity Standards. The National Institute for Standards and Technology (NIST) worked with the private sector to create a Cybersecurity Framework with voluntary standards and practices to promote the protection of critical infrastructure. These standards represent best practices for responsible cybersecurity management of critical infrastructure to understand and mitigate cybersecurity risks. In 2018, GAO reviewed efforts by Federal agencies to promote awareness and adoption of the NIST Cybersecurity Framework among owners and operators of critical infrastructure, including transportation infrastructure.

GAO found that the Department of Transportation and the Department of Homeland Security had worked to promote awareness and use of the framework applied to critical infrastructure, but that the agencies did not have information to know the extent of adoption within the transportation sector. GAO recommended that both agencies take steps to determine the level and type of framework adoption across critical infrastructure in the transportation sector.

Question 3. What has DOT done to implement this recommendation to understand to degree to which transportation entities have implemented the NIST Cybersecurity Framework?

Answer. DOT and the Department of Homeland Security (DHS) are Co-Sector Risk Management Agencies (Co-SRMAs) for the Transportation Systems critical infrastructure sector (Sector), meaning they share responsibility for using specialized expertise to support Sector risk management, establish and carry out programs to assist critical infrastructure owners and operators, and facilitate information sharing among other duties. In addition to efforts DOT Operating Administrations took to promote the adoption of NIST Cybersecurity Framework with critical infrastructure stakeholders, the Co-SRMAs incorporated discussion and promotion of the framework throughout various Sector-related stakeholder engagements.

Furthermore, the Co-SRMAs developed a draft survey to determine the level and type of framework adoption within the Sector, and the Co-SRMAs shared the draft survey with Sector Coordinating Council (SCC) leads and Sector stakeholders in May 2020 to seek voluntary comments that would inform how the Co-SRMAs finalized the survey.

In March 2021, the Co-SRMAs shared the final survey with SCC leads and Sector stakeholders so they had opportunity to complete the survey voluntarily, and the Co-SRMAs requested their voluntary assistance in distributing the survey as broadly as possible within the Sector. The Co-SRMAs are working on a report of the sur-

vey findings that may include recommendations the Co-SRMAs can consider to increase awareness and adoption of the framework.

Question 4. Should the practices outlined in the NIST Cyber Security Framework be made mandatory for transportation industries?

Answer. Cybersecurity by nature is a dynamic and evolving field. As noted in the NIST Framework, the Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks—different threats, different vulnerabilities, different risk tolerances. Transportation critical infrastructure entities are encouraged to use the Framework; however, mandating frameworks may cause unintended consequences. While there is no coordinated requirement for cybersecurity across all critical infrastructure, including the transportation industries, cybersecurity standards and frameworks, such as the NIST Cyber Security Framework, should be utilized to establish baseline practices that owners and operators can follow to protect national and economic security, as well as public health and safety.

Manual Operation of Pipelines. There was enormous pressure to get the Colonial Pipeline back up and running after the ransomware attack. To expedite this process Colonial decided to manually operate the pipeline. This required people to physically open and close valves at a number of different locations to get different products from one place to the next. It is my understanding that this process is extraordinarily rare in modern times and requires a number of highly trained operators to work around the clock.

Question 5. What processes does PHMSA currently have in place to ensure the manual operation of a pipeline in response to an emergency is safe?

Answer. If a pipeline company chooses to operate in manual mode, appropriate procedures must be in place by operators or be established prior to implementation of manual operations. Additionally, personnel must be qualified to perform the manual operation functions. Per 49 C.F.R. § 192.605 and § 192.615, pipeline operators must prepare a manual of written procedures for normal operations, maintenance operations, and emergency response. With the widespread deployment of electronically managed pipeline systems, there has been a sharp decline in the utilization of manual operations. In response to the recent Colonial Pipeline cybersecurity event, PHMSA is reviewing pipeline companies' preparedness to respond to, and safely recover from, a cyber-attack, including the potential need for manual operation of all or portions of its facilities.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TAMMY DUCKWORTH TO
HON. POLLY TROTTEMBERG

GPS Resiliency and Backup. The U.S. Global Positioning System (GPS) is critically important to our nation, providing position, navigation and timing (PNT) services that underlie our economic and national security. Sixteen critical infrastructure industries rely on GPS for PNT, including telecommunications, electrical grid, public safety, aviation and auto industries. A study by the National Institute of Standards and Technology (NIST) found that GPS has an overall economic impact of \$700-\$800 billion and is doubling every two to three years.

Unfortunately, GPS systems elsewhere in the world are increasingly threatened by disruption, jamming, and attacks by malicious actors. As co-chair of the Senate GPS Caucus, it is apparent to me that continuing GPS modernization and resiliency efforts that ensure our system continues to be the world's PNT gold standard is vitally important.

Dating back to 2004, Congress and the Executive Branch expressed interest for establishing or improving GPS resiliency. Defense authorization legislation enacted in 2017 and 2018 tasked USDOT, DHS and DOD with developing a GPS backup strategy and an Executive Order was issued on PNT resilience recommending a combination of systems to increase GPS resiliency. In 2018, the National Timing Resilience and Security Act (NTRSA) was enacted to support the deployment of a land-based GPS backup.

Executive Order 13905 in February 2020 followed by a January 2021 report by USDOT, in conjunction with DOD and DHS, affirmed the Federal perspective that no one technology can address all potential use cases and a nationwide backup requires a combination of technologies.

Question 1. What steps is USDOT taking to implement the recommendations of the January 2021 report and to procure GPS backup technologies based on the report's recommendations? Is USDOT advancing demonstration efforts highlighted in

its report to ensure the U.S. has available a full backup system for PNT services across our critical infrastructure?

Answer. DOT's Office of the Assistant Secretary for Research and Technology (OST-R), through work authorized and funded under the FY 2018 National Defense Authorization Act (NDAA), has demonstrated suitable and mature PNT technologies that can complement GPS and could provide a backup to GPS/Global Navigation Satellite System (GNSS) service in case of a major disruption. Many of these technologies are already commercially available for owners and operators of critical infrastructure to utilize (particularly for timing). In many of these most critical infrastructure sectors that rely on timing, it is the financial cost associated with these alternate systems that hampers adoption. GPS and the foreign GNSS systems are provided free of direct user fees. Despite the known vulnerabilities with GPS/GNSS, most users are unwilling to adopt other available PNT systems because they are only available for a fee. Barring economic justifications, regulatory requirements or incentives, adoption of alternate PNT systems will remain limited.

However, recognizing that the transportation sector has some of the most stringent performance requirements for both positioning and navigation, as well as timing, in terms of accuracy, integrity, availability, and reliability, DOT is developing system requirements that focus on safety and resilience. These system requirements will allow determination of which PNT performance requirements can be currently met and which requirements may require further innovation.

Based on recommendations from the DOT Complementary PNT Demonstration Report to Congress submitted in January 2021 (<https://www.transportation.gov/briefing-room/us-dot-releases-complementary-positioning-navigation-and-timing-pnt-and-gps-backup>), there are three components in the President's FY 2022 budget request for DOT to pursue:

1. Development of safety-critical PNT standards for transportation services.
2. Development of a PNT vulnerability and performance testing framework on demonstrated and suitable complementary technologies.
3. Development of PNT performance monitoring capabilities to ensure PNT services provide operational resilience and achieve safety-critical standards.

These efforts will further develop PNT modeling, simulation, and testing tools, as well as standards and performance monitoring tools. These capabilities are needed to evaluate integration of diverse positioning, navigation, and/or timing technologies and will facilitate successful transition and adoption into end-user applications.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. KYRSTEN SINEMA TO
HON. POLLY TROTTENBERG

Cybersecurity Workforce at the Department of Transportation. The Senate Commerce, Science and Transportation Committee hearing spent some time discussing the challenges of obtaining and retaining qualified cyber security experts within the Federal government. I understand that the Department of Transportation (DOT) is currently working on a Government Accountability Office (GAO) recommendation to identify all cybersecurity occupations across the agency to better assess whether any changes are needed to DOT's workforce planning efforts (GAO-21-197).

Question 1. Can provide any general findings as to what degree gaps in this skill field are hindering the agency's ability to effectively oversee all aspects of the U.S. transportation system?

Answer. Ensuring that the Department has a workforce with the skills and competencies to meet the challenges of the future is a priority for DOT. The Department's Highly Automated Systems Safety Center of Excellence (HASS COE) is currently working with each DOT Operating Administration to determine their current automation workforce status, needs, and plans. In partnership with the DOT Office of Human Resources, the assessments will determine competencies and assess skill gaps in key occupational groups that are involved in overseeing the safety of automated technologies. We will use the results of the assessments, along with our workforce planning efforts, to work with all of our Operating Administrations to address the recommendations in the GAO report.

Further, the FAA is part of a jointly led Aviation Cyber Initiative that partners with the Department of Homeland Security and Department of Defense. The focus is on addressing cybersecurity risk to the Nation's Aviation Ecosystem to support the National Strategy for Aviation Security (NSAS). FAA manages cybersecurity threats to the national airspace system through a cybersecurity steering committee

that manages risks and training through annual updates to the FAA Cybersecurity Strategy. These efforts will help DOT better understand the impacts on the overall U.S. transportation system.

Question 2. Aside from the talent gap, what other key challenges on the cybersecurity front does DOT face in overseeing and enforcing pipeline control room regulations, integrity management plan requirements, and emergency response plan regulations?

Answer. A key challenge is the need to increase awareness throughout the entire industry of the risk of cyber-attacks and each company's vulnerability to those attacks. Many companies, especially smaller or lower profile facilities, may not believe they are at risk or consider minimal protections as adequate. Further, without specialized training, it is difficult for Federal and state inspectors to identify cyber—and therefore potential safety and/or environmental risks—on pipeline facilities. Cyber related attacks can directly result in pipeline failures, releasing hazardous materials and potentially harming people and the environment. PHMSA has requested increased funding in its FY 2023 budget to provide cyber awareness training to more Federal and state inspectors. Increasing awareness and training of cyber vulnerabilities and what constitutes good cyber hygiene among industry and Federal/state agencies is critical to improving the protection of the Nation's infrastructure.

DOT preparedness to Respond to Cyber Attacks. Recent cyberattacks affecting our Nation's gasoline supply serve as a reminder that virtually every industry is vulnerable to cyber events.

Question 3. In addition to Pipeline Systems, how would DOT grade its preparedness to respond to and mitigate significant cyber events in other key Transportation Systems subsectors—such as aviation, highway and motor carrier, maritime, mass transit and passenger rail, freight rail, and postal and shipping? Are there any lessons learned from recent events over improving the cyber response and resilience to pipeline systems that should be implemented in the other subsectors?

Answer. Since DOT and DHS are Co-SRMAs for the Transportation Systems critical infrastructure sector, DOT's preparedness to respond to and mitigate significant cyber events across the Sector—regardless of which subsector listed is impacted—centers largely on the Co-SRMAs' efforts to fulfill the SRMA role, in coordination with the Cyber Unified Coordination Group (UCG), as prescribed in Presidential Policy Directive (PPD) 41, United States Cyber Incident Coordination, released in 2016. Per PPD-41, the Co-SRMAs developed enhanced coordination procedures to prepare for situations related to critical infrastructure in which the demands of a significant cyber incident exceed one department or agency's capacity. DOT and DHS tested these procedures during the biennial Cyber Storm exercise in 2018. For its part, DOT will update its enhanced coordination procedures in 2022, in coordination with DHS.

Regarding lessons learned, as personnel can change from one year to the next, the Department realized the need to solidify and emphasize DOT's internal understanding of the unique response or mitigation elements associated with a cyber incident response. These elements can differ significantly depending on the circumstances from more "traditional" response measures associated with physical incidents, such as hurricanes. In turn, following the Cyber Storm exercise, and as part of DOT's internal efforts to streamline its incident response plans, DOT developed a Cyber Annex to DOT's 2020 "All Threats, All Hazards Response and Recovery Deliberate Plan." The 2020 Annex includes some interagency actions and updates to PPD-41 requirements, which apply to pipeline systems as well as other subsectors.

Question 4. If DOT receives notice of a cyberattack or a ransomware payment from a pipeline owner or operator, what is your understanding of the interagency process for coordinating efforts amongst key Federal agencies? If DOT is notified rather than CISA, would DOT experts know how to start the interagency coordination process amongst key stakeholders to quickly gather information and respond to the attacks?

Answer. If DOT directly received such a notice, the immediate step is to ensure that the owner or operator report such incidents to the DHS Cybersecurity and Infrastructure Security Agency (CISA). DOT, when made aware, also notifies CISA. In addition, PPD-41 outlines the standing process for interagency coordination among key Federal agencies related to critical infrastructure.

Furthermore, as Co-SRMAs for the transportation systems sector, DOT and DHS (through the Transportation Security Administration (TSA) and the United States Coast Guard (USCG)) have a strong, long-standing relationship that exemplifies how the Federal Government builds trusted partnerships and advances a national unity of effort to strengthen and maintain a secure, functioning, and resilient trans-

portation sector. The Co-SMRAs play a critical role in sharing of threat and intelligence information, as well as other information and products, which directly supports the implementation of PPD–21, PPD–41, and Executive Orders on cybersecurity.

TSA has the authority to issue Security Directives (SDs) and has used this authority to issue several SDs. In turn, the Transportation Security Oversight Board (TSOB)¹ authorizes the effective timeframes of the SDs. TSA initially released SD Pipeline-2021–01 in May 2021—amended in December 2021 and effective through May 28, 2022—which requires pipeline owners and operators to report cybersecurity incidents to CISA when they involve systems that the owner/operator has responsibility to operate and maintain.

TSA issued a complementary SD—mandating that critical owners and operators of gas and liquid pipelines implement an array of cybersecurity measures to prevent disruption and degradation to their infrastructure—in July 2021 (amended in December 2021) that is effective through July 26, 2022. This SD generally requires owners and operators to: 1) implement critically important mitigation measures to reduce the risk of compromise from a cyberattack; 2) develop a Cybersecurity Contingency/Response Plan to reduce the risk of operational disruption or significant business or functional degradation of necessary capacity should the Information and/or Operational Technology systems of a gas or liquid pipeline be affected by a cybersecurity incident; and 3) evaluate and validate the cybersecurity of their ICS networks through an annual validated architecture design review.

TSA also published two SDs in December 2021, SD 1580–2021–01 and SD 1582–2021–02, for higher risk railroads and rail transit owner/operators that require measures to improve cybersecurity preparedness including appointment of cybersecurity coordinators, reporting of cybersecurity incidents to CISA, conducting a cybersecurity vulnerability assessment, and development of cybersecurity incident response plans. TSA also distributed an Information Circular, IC–2021–01, recommending the same measures for lower risk railroads, public transportation, and over-the-road buses, followed by a similar Information Circular for pipeline entities beyond those addressed in the first two pipeline SDs.

DOT supported the review and development of these SDs and supported coordination for stakeholder engagements with industry to provide information and solicit feedback and questions on the SDs. Further, DOT serves as a principal member of the TSOB, led by DHS and established under the Aviation and Transportation Security Act, to provide guidance regarding transportation security-related matters. As a TSOB member, DOT is responsible for reviewing and ratifying or disapproving emergency regulations or security directives issued by TSA, including the recently issued pipeline security directives. In light of DOT's Co-SRMA role alongside DHS and TSOB membership, DOT regularly coordinates with DHS/TSA counterparts and is well-positioned to prompt and establish necessary interagency coordination processes amongst key stakeholders to facilitate quick information sharing and response.

DOT is also aware that TSA has significantly increased its cybersecurity expertise through hiring and focusing resources to support cybersecurity enhancements for all modes of transportation.

TSA under its Surface Operations program component has established its own Cybersecurity Branch which has been staffed with a team of 11 cybersecurity experts that possess expert level technical skills and unique specialized cyber experience to support surface cross-modal cybersecurity efforts. This newly established unit will allow TSA to carry-out a number of both timely and critical cybersecurity related functions to enhance the security and resilience of the surface transportation system sector, as well as advance other TSA cyber-related mission requirements.

TSA's cybersecurity subject matter experts have specialized knowledge and experience related to Operational Technology/Industrial Control Systems (OT/ICS) networks, vulnerability analysis, cyber incident analysis and mitigation, assessments, and defense. This aforementioned expertise has been obtained through their experience with cybersecurity industry leaders such as DHS, CISA, U.S. Department of Defense (DoD), and U.S. Department of Energy (DoE), Idaho National Laboratory (INL). Additionally, these candidates bring a variety of industry-recognized cybersecurity certifications to TSA Surface Operations from the SysAdmin, Audit, Network, and Security (SANS) Institute, various Global Information Assurance Certifications (GIACs), and other relevant organizations.

¹ 49 U.S.C. § 115(c)(1); 49 U.S.C. § 114(l)(2)(B).

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RON JOHNSON TO
HON. POLLY TROTTERBERG

Background: According to a 2018 Department of Transportation (DOT) report, pipelines are a safer mode of transportation for shipping oil than truck and rail. However, due to President Biden's revocation of the Presidential Permit for the Keystone XL pipeline, Canadian oil will likely enter the U.S. market by rail and trucks.

Question 1. Could you please state whether transporting oil by pipeline continues to be a safer mode of transportation?

Answer. On January 20, 2021, President Biden revoked the March 29, 2019 Presidential permit for the Keystone XL pipeline, finding that it does not serve the U.S. national interest and that leaving the Keystone XL pipeline permit in place would not be consistent with the Administration's economic and climate imperatives.

Pursuant to a directive from Congress, in 2018, the Pipeline Hazardous Materials Safety Administration (PHMSA) produced a *Report on Shipping Crude Oil by Truck, Rail, and Pipeline*. The report includes safety data by year and by mode, including total incidents, spill rates, serious injuries, and fatalities and is available here: <https://www.phmsa.dot.gov/sites/phmsa.dot.gov/files/docs/news/70826/report-congress-shipping-crude-oil-truck-rail-and-pipeline-32019.pdf>.

According to the report, shipping oil by pipeline is safer than other modes of transportation based on comparisons of certain safety indicators, including percent spilled and incident rate. The report does indicate that other modes of transportation would be considered safer than pipelines if human consequences are the main indicator. However, the relative comparison of serious injuries and fatalities between modes demonstrates that there is relatively no difference between modes because serious injuries and fatalities are extremely rare.

Follow-up. Could you please provide DOT's estimates for how revoking the permit may affect the traffic fatalities from increased road congestion and accidents?

Answer. DOT does not have estimates of this nature.

Question 2. Did DOT conduct an economic impact analysis on the impact of revoking the Keystone XL pipeline permit? If yes, could you please provide DOT's estimates for how revoking the permit may affect truck and rail transportation costs?

Answer. No.

Follow-up. Could you please explain how this decision may affect timeliness and delays for current freight traffic schedules? Additionally could you please provide DOT's estimates for how revoking the permit may affect freight and road traffic congestion?

Answer. N/A.

Background: President Obama's State Department issued environmental reviews that found no major environmental objections to the pipeline on five separate occasions and that alternative methods to get oil from Canada to Gulf state refineries are worse for climate change.

Question 1. Do you agree with President Obama's State Department's assessment? If not, please explain.

Answer. Congress has granted PHMSA with authority to review pipeline design, and to monitor the construction, operations, and maintenance of pipelines. Congress has granted other agencies and departments the role of reviewing siting decisions, energy market dynamics, and, environmental impacts. In light of President Biden's revocation of the March 29, 2019 Presidential permit for the Keystone XL pipeline, DOT does not have plans to review previous Department of State assessments.

Question 2. Could you please state whether transporting oil by pipeline is a more environmentally friendly mode of transportation than by rail or truck?

Answer. Transporting oil by pipeline allows for greater volumes to be moved longer distances more quickly and efficiently than by rail or truck; however, pipeline spills tend to be far greater in size than rail car or truck spills. Comparability is further hampered by differences in incident-reporting criteria between the modes.

Question 3. Could you please provide DOT's estimates for any increase for oil leaks or spills from using potentially more risky modes of transportation like truck and rail?

Answer. DOT focuses on safety in all modes of transportation. Because each mode has its own unique incident causes related to oil spills—from operator error to mechanical defect to third-party damage, it is difficult to make comparative predictive studies of potential spills. Using the compiled information in the aforementioned 2018 *Report on Shipping Crude Oil by Truck, Rail, and Pipeline*, which is the most readily available data, the spill percentage, i.e., volume spilled per volume transported for 2014, 2015 and 2016¹ were:

Spill Percentage (volume spilled per volume transported)

	Pipeline	Rail	Truck
2016	0.0011%	0.0008%	0.0003%
2015	0.0006%	0.0116%	0.0009%
2014	0.0005%	0.0009%	0.0016%

As seen above, the percentages varied widely by year as is common in low frequency, high consequence industries.

Question 4. Did DOT conduct any analyses examining the environmental impact from revoking the permit for the Keystone XL pipeline?

Answer. No. The revocation was not a DOT action necessitating a DOT environmental review.

Follow-up: If yes, could you please provide details of the analyses such as the estimated change in greenhouse gas emissions and temperature due to replacing pipeline use with rail and truck use?

Answer. N/A.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARSHA BLACKBURN TO
LESLIE V. GORDON

Background: During the hearing, you talked about GAO's recommendations to TSA. Specifically, the recommendation for TSA to seek more comprehensive data information from sources beyond just pipeline operators to contribute to better assessing the cyber threat environment.

Question. What specific types of data does GAO believe would be helpful for TSA to collect?

Answer. In our December 2018 report, we identified several factors that likely limit the usefulness of TSA's risk assessment in effectively prioritizing TSA security reviews of pipeline systems.¹ Specific to cybersecurity information, we found that the risk assessment did not include a measure of cybersecurity vulnerabilities. According to Pipeline Security Branch officials, absent data specific to pipelines on their cyber vulnerabilities, they were unable to include a pipeline's vulnerability to cyberattack in their risk assessment. In our report, we stated that developing a feedback mechanism between TSA and pipeline operators based on their implementation of TSA's Pipeline Security Guidelines—including those on cybersecurity—could be an important input into TSA's risk assessment's vulnerability calculation. This information would also inform the amount of risk pipeline companies are reducing by implementing the guidelines and could be used to inform overall risk reduction. In addition, we found that TSA's risk assessment did not include threats to cybersecurity, such as data on prior attacks. According to National Institute of Standards and Technology (NIST) risk management guidance, although risk models differ in the degree of detail and complexity with which threats are factored, threats are a foundational element for all cybersecurity risk models.²

Similarly, in February 2018 and February 2020, we found that the Department of Transportation (DOT) and DHS had not developed methods for determining the level and type of adoption of the NIST *Framework for Improving Critical Infrastructure Cybersecurity* by entities across the transportation sector—including the pipeline subsector.³ We concluded that, until DOT and DHS have a more comprehensive understanding of the use of the cybersecurity framework by entities within the Transportation sector, they will be limited in their ability to understand the success of protection efforts or to determine where to focus limited resources for cyber risk mitigation. We made two recommendations that DOT, in coordination with DHS, should take to address these weaknesses. DOT agreed with the recommendations but has not yet addressed them.

¹ GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management*, GAO-19-48 (Washington, D.C.: Dec. 18, 2018).

² NIST, *Guide for Conducting Risk Assessments*, Special Publication 800-30 Revision 1 (Gaithersburg, M.D.: Sept. 2012).

³ GAO, *Critical Infrastructure Protection: Additional Actions Needed to Identify Framework Adoption and Resulting Improvements*, GAO-20-299 (Washington, D.C.: Feb. 25, 2020); *Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption*, GAO-18-211 (Washington, D.C.: Feb. 15, 2018).

Follow-up. Does the absence of any of these data sources suggest that the TSA was hasty in adopting the two security directives?

Answer. The absence of cybersecurity vulnerability data sources does not necessarily suggest that TSA was hasty in adopting its May and July 2021 security directives. The security directives require pipeline operators to take certain measures to address cybersecurity vulnerabilities, whereas the cyber risk information referred to above is to be used by TSA to prioritize its resources when conducting TSA security reviews of pipeline systems. However, we have not reviewed TSA's decision to require that certain pipeline owners and operators implement cybersecurity practices as part of the second security directive. When making such requirements, it is important that agencies fully consider the cybersecurity risks—including the likelihood of cyberattacks and their potential impact—what cybersecurity practices are needed to address those risks, and the costs that implementing these practices will impose on the owners and operators.

