



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 2015. 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 curriec@gao.gov and Nick Marinos at (202) 512-9342 or marinosn@gao.gov.

December 2018

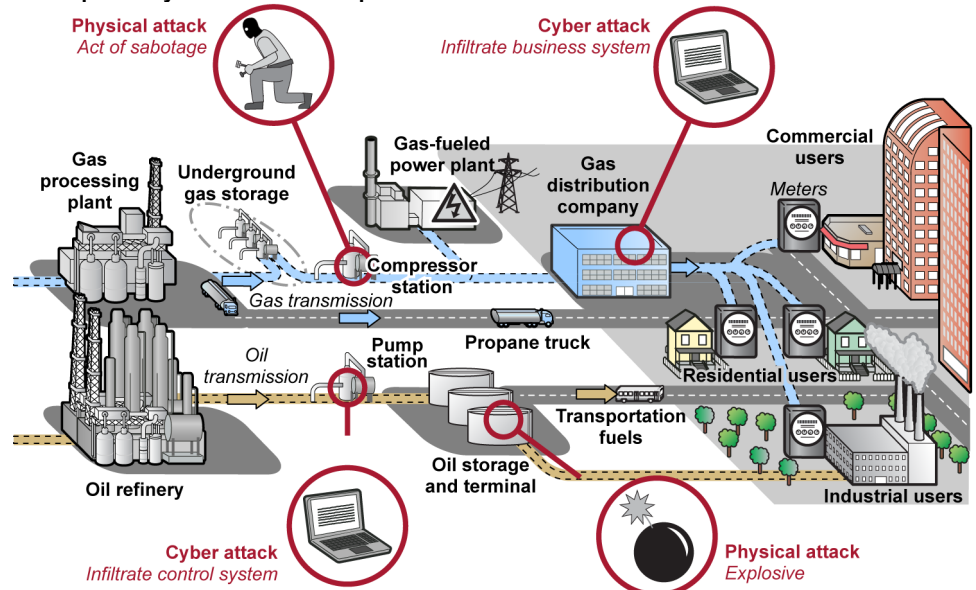
CRITICAL INFRASTRUCTURE PROTECTION

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

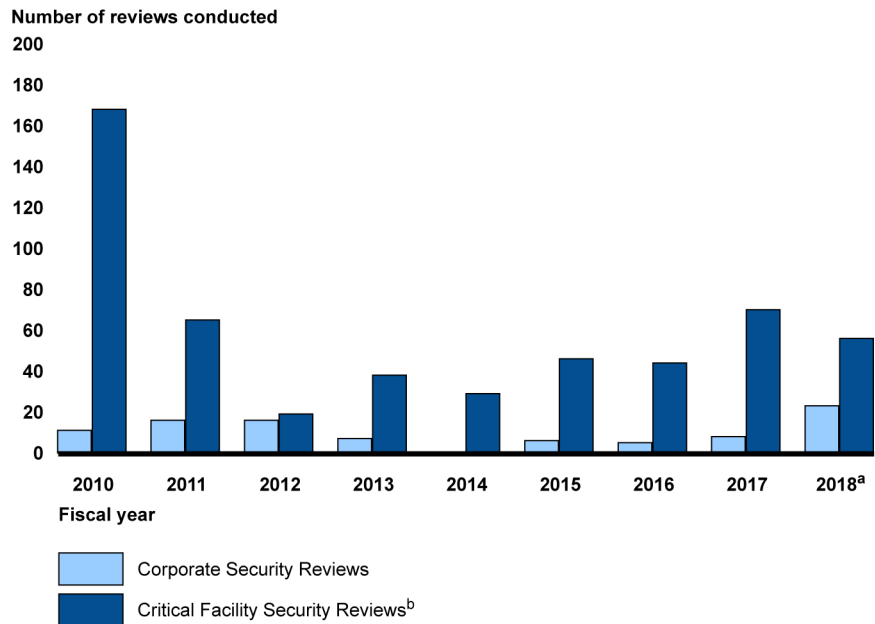
To assess pipeline security risks, TSA conducts pipeline security reviews—Corporate Security Reviews and Critical Facility Security Reviews—to assess pipeline systems' vulnerabilities. However, GAO found that the number of TSA security reviews has varied considerably over the last several years, as shown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

Contents

| | | |
|--------------|--|----|
| Letter | | 1 |
| | Background | 7 |
| | Federal and Non-federal Pipeline Stakeholders Exchange Risk-Related Security Information | 23 |
| | 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 | 27 |
| | TSA Assesses Pipeline Risk and Conducts Security Reviews, but Limited Workforce Planning and Shortfalls in Assessing Risk Present Challenges | 36 |
| | TSA Has Established Performance Measures, but Limitations Hinder TSA’s Ability to Determine Pipeline Security Program Effectiveness | 48 |
| | Conclusions | 60 |
| | Recommendations for Executive Action | 62 |
| | Agency Comments and Our Evaluation | 63 |
| Appendix I | Federal and Industry Security Guidelines and Standards for the Pipeline Sector | 69 |
| Appendix II | Description of Areas for Improvement in the Pipeline Security Branch’s Pipeline Relative Risk Ranking Tool | 70 |
| Appendix III | Comments from the Department of Homeland Security | 79 |
| Appendix IV | GAO Contact and Staff Acknowledgments | 85 |
| Tables | | |
| | Table 1: Federal Information Sharing Entities and Programs that Provide Information to Pipeline Stakeholders | 24 |
| | Table 2: Non-federal Information Sharing Entities | 26 |
| | Table 3: TSA Pipeline Staffing Levels, Fiscal Years 2010 through 2018 | 39 |
| | Table 4: Shortfalls in the Pipeline Security Branch’s Risk Ranking Assessment | 43 |

| | |
|---|----|
| Table 5: 2018 NSTS Pipeline Security Plan Performance Measures, Goals 1 and 2 | 50 |
| Table 6: Management Measure in DHS FY2019 Congressional Budget Justification | 51 |
| Table 7: Key Attributes of Effective Performance Measures | 52 |
| Table 8: Federal and Industry Guidelines and Regulations Identified as Applicable to Security by the Pipeline Operators | 69 |

Figures

| | |
|--|----|
| Figure 1: Map of Hazardous Liquid and Natural Gas Transmission Pipelines in the United States, September, 2018 | 8 |
| Figure 2: U.S. Natural Gas and Oil Pipeline Systems' Basic Components and Vulnerabilities | 10 |
| Figure 3: The National Infrastructure Protection Plan's Critical Infrastructure Risk Management Framework | 16 |
| Figure 4: Determination of Risks Related to Infrastructure Protection | 16 |
| Figure 5: Overview of the Transportation Security Administration's (TSA) Voluntary Security Review Processes with Pipeline Operators | 20 |
| Figure 6: Timeline of Federal Pipeline Security Guidelines Development | 31 |
| Figure 7: Pipeline Security Reviews Conducted, FY2010 through FY2018 YTD | 38 |

Abbreviations

| | |
|-------|---|
| AGA | American Gas Association |
| API | American Petroleum Institute |
| CFSR | Critical Facility Security Reviews |
| CRISP | Cybersecurity Risk Information Sharing Program |
| CSR | Corporate Security Reviews |
| DHS | Department of Homeland Security |
| DOE | Department of Energy |
| DOT | Department of Transportation |
| FERC | Federal Energy Regulatory Commission |
| ICS | Industrial Control Systems |
| INGAA | Interstate Natural Gas Association of America |
| ISAC | Information Sharing and Analysis Center |
| NCCIC | National Cybersecurity and Communications Integration Center |
| NIPP | National Infrastructure Protection Plan |
| NIST | National Institute of Standards and Technology |
| NSTS | National Strategy for Transportation Security |
| NTAS | National Terrorism Advisory System |
| OEIS | Office of Energy Infrastructure Security |
| PHMSA | Pipeline and Hazardous Materials Safety Administration |
| SCADA | Supervisory Control and Data Acquisition |
| SCC | Sector Coordinating Council |
| TSA | Transportation Security Administration |
| TSOC | Transportation Security Operations Center |

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



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

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.

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

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).

critical facility 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.,

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.

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 security-related standards and guidance they use and asked them about any challenges they experienced in implementing

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.

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

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

¹⁴To 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.

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

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

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

¹⁷GAO, *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).

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

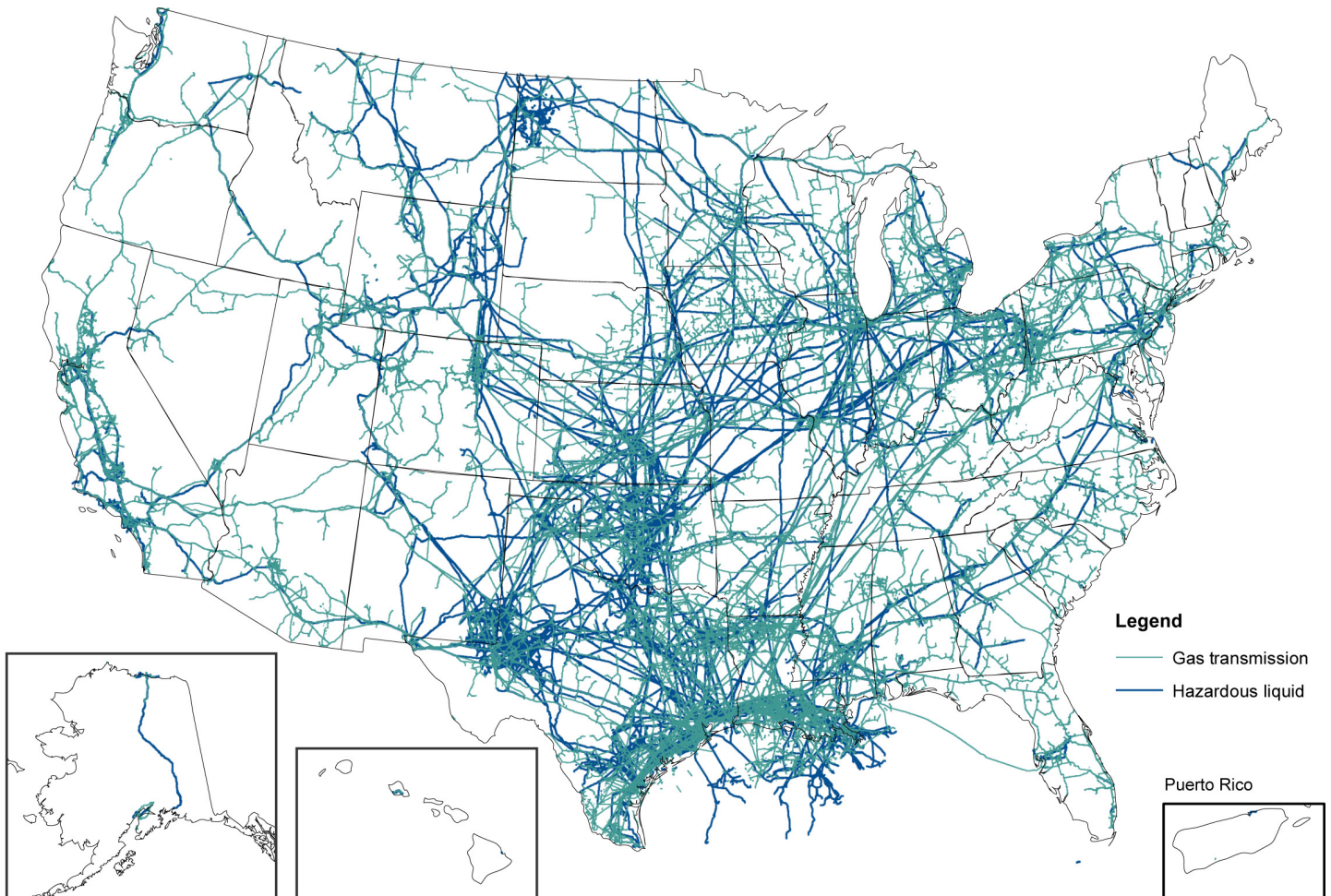
Overview of the U.S. Pipeline System

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 intrastate—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



Source: U.S. Department of Transportation. | GAO-19-48

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,

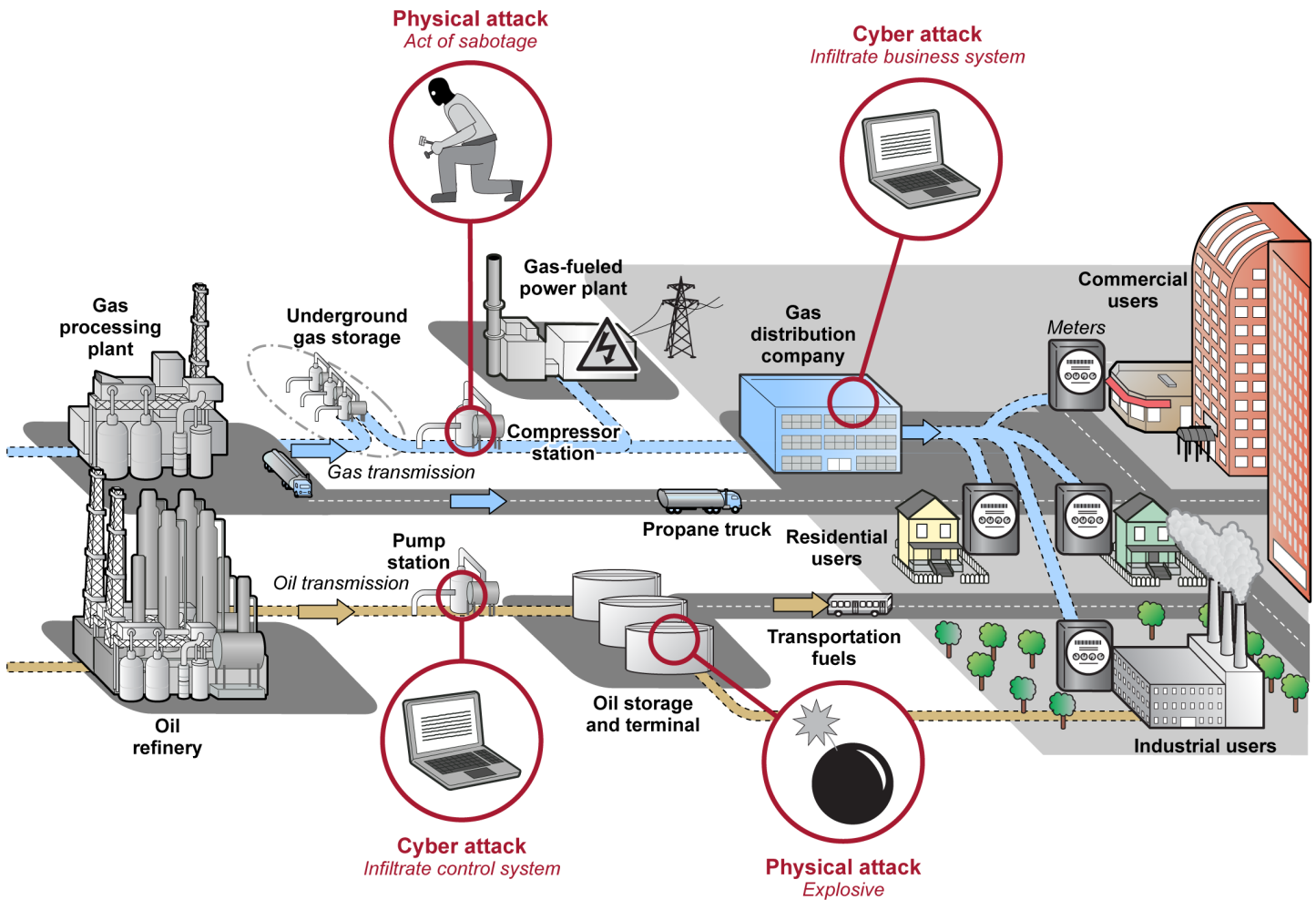
signals, and preprogramed parameters to activate and deactivate valves and pumps to maintain flows within tolerances.¹⁸

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.

¹⁸SCADA 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—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](#).

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 attacking 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

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

²¹For 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. Assaults 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 Congressional Research Service, *Pipelines: Securing the Veins of the American Economy*, TE10009 (Washington, D.C.: Apr. 19, 2016).

²²In 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.

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

²⁴Once 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).

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.

²⁵NCCIC 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.

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

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

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, explosions, 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

²⁸In 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 emails 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 rebooting.

²⁹"Spear-phishing" involves sending official-looking emails 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.

³⁰NCCIC 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)).

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

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 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

³²White 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.

³³The 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.

³⁴PPD-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.

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

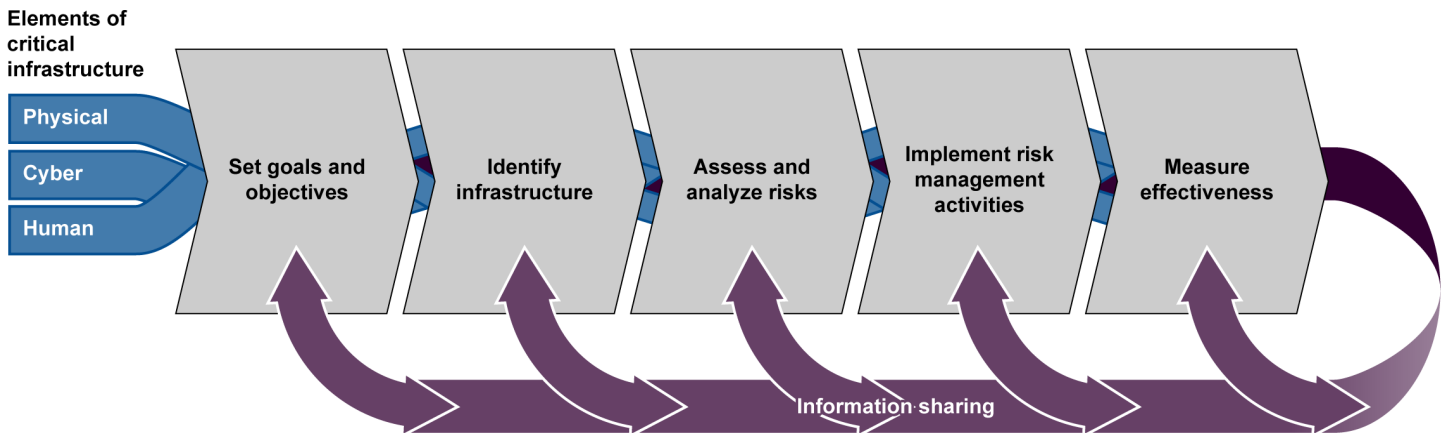
The NIPP also outlines a risk management framework for critical infrastructure protection. As shown in Figure 3, the NIPP uses a risk management framework as a planning methodology intended to inform how decision makers take actions to manage risk. The risk management framework calls for public and private 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.

³⁵Government 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.

³⁶SCCs 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.

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

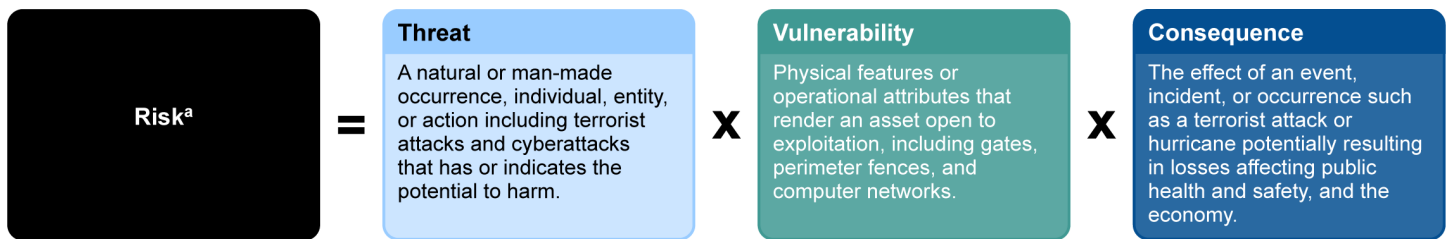
Figure 3: The National Infrastructure Protection Plan’s Critical Infrastructure Risk Management Framework



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

^aAs 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 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

³⁸Among 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 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.

³⁹Exec. 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).

⁴⁰Exec. 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.

⁴¹National 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).

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

⁴²Pursuant 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).

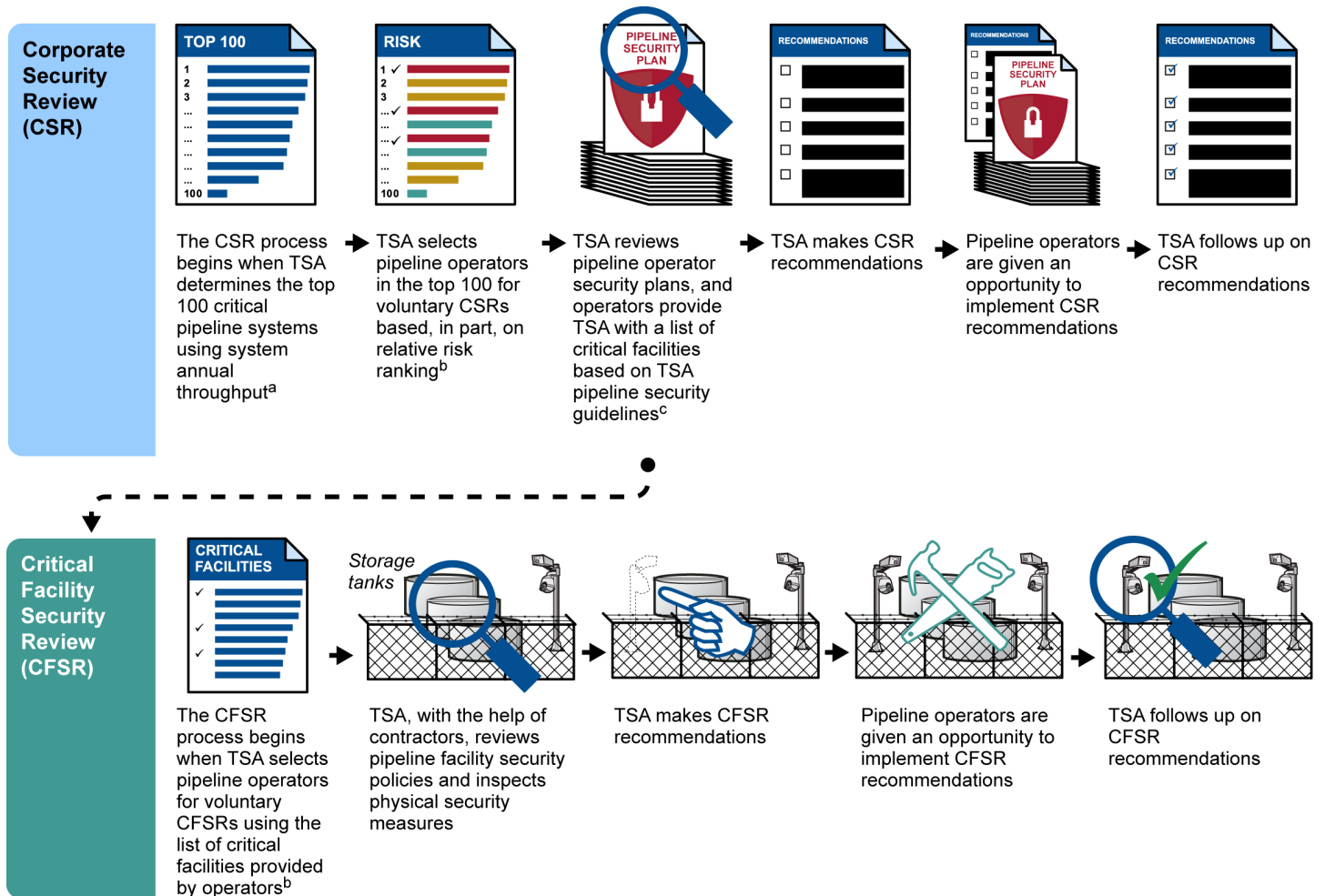
⁴³The Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act) directs the Secretary of Homeland Security, in conjunction with the Secretary of Transportation, to develop and transmit to pipeline operators security recommendations for natural gas and hazardous liquid pipelines 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.

⁴⁴See 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.

in the report. Additionally, TSA's Pipeline Security Branch is responsible for conducting voluntary Corporate Security Reviews (CSR) and Critical 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.

⁴⁵CSRs 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.

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 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

⁴⁶According 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.

⁴⁷National 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.

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.

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

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.

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 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

⁵³[GAO-10-867](#).

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 |
|--|--|
| Department of Homeland Security (DHS) | |
| National Cybersecurity and Communications Integration Center (NCCIC) | 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 |
| Transportation Security Administration (TSA) Transportation Security Operations Center (TSOC) | 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. |
| TSA Intelligence and Analysis | 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. |
| National Terrorism Advisory System (NTAS) | 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.e., general information about timing and target) or imminent (i.e., credible, specific, and impending) threats. |
| Homeland Security Information Network (HSIN) | 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. |
| Protective Security Advisor (PSA) Program | 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. |
| Department of Transportation (DOT) | |
| Pipeline and Hazardous Materials Safety Administration (PHMSA) | 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 |

| Entity/Program | Product/service description |
|---|---|
| Department of Energy (DOE) | |
| Cybersecurity Risk Information Sharing Program (CRISP) | 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. |
| Federal Energy Regulatory Commission (FERC) | |
| Office of Energy Infrastructure Security (OEIS) | 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

³NCCIC 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 email 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

⁵⁴According 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.

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.

Table 2: Nonfederal Information Sharing Entities

| Entity | Product/service description |
|--|--|
| Downstream Natural Gas Information Sharing and Analysis Center (ISAC) | 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. |
| Oil and Natural Gas ISAC | 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. |
| Fusion centers | 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. |
| Industry associations | 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. |
| InfraGard | 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. |
| Oil and Natural Gas Subsector Coordinating Council (SCC) | 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

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.

⁵⁵See 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 Security

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

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,

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).

guidelines, and practices that may be scaled and applied to address a pipeline operator's cybersecurity risks.⁶¹

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-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

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.

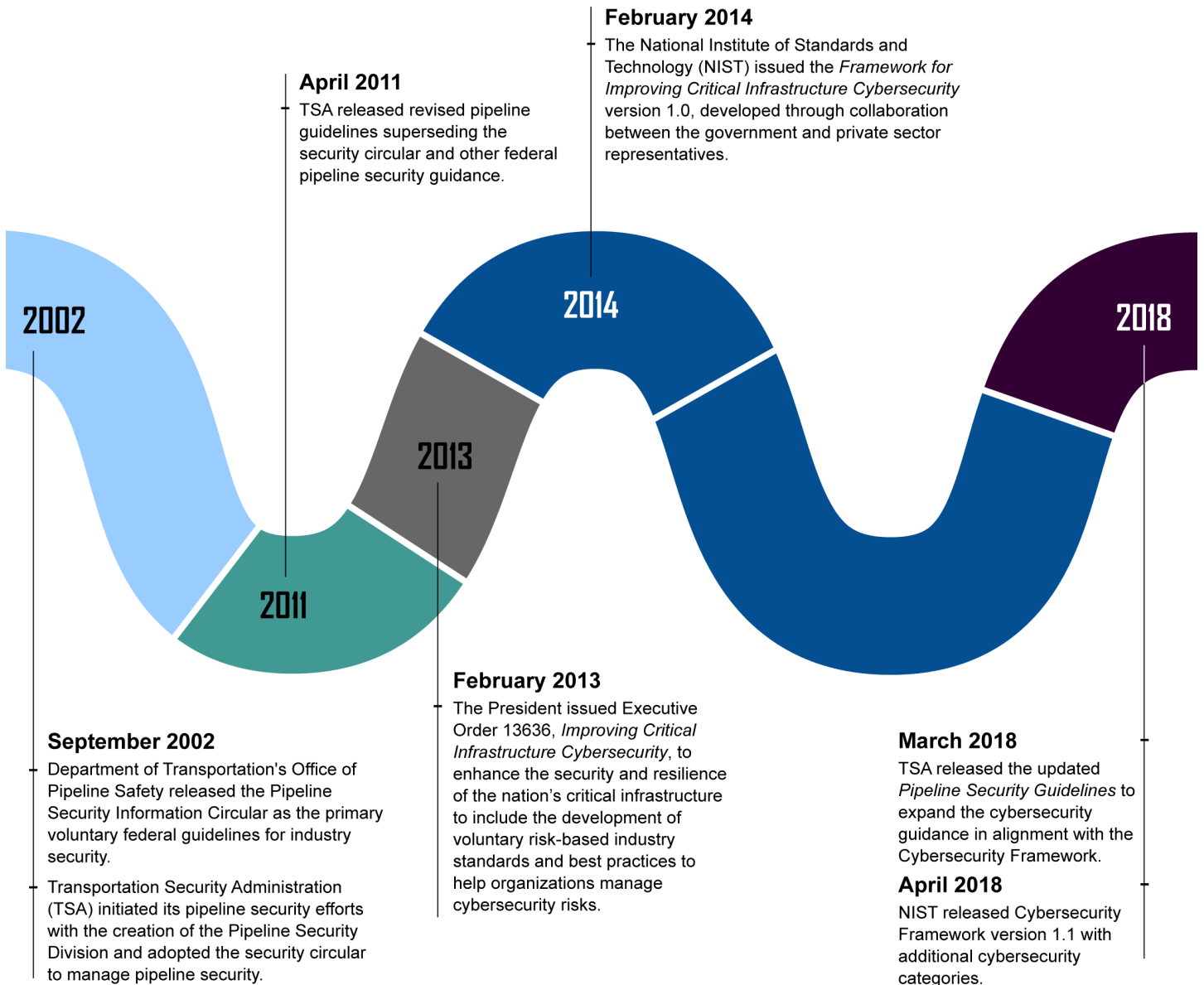
⁶²See 49 C.F.R. pts. 190-199.

⁶³See 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.

⁶⁴Maritime 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.

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

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

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

⁶⁶[GAO-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."

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

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

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 operators 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

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

TSA's criteria were not clear, they created their own criteria which helped the operator identify two additional critical facilities.

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

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

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 officials, 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

⁷⁰According 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.

⁷¹According 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.

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



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

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

^bFiscal 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

⁷²In 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

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.

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 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

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).

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.

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).

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.

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](#).

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 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 | <ul style="list-style-type: none"> <li data-bbox="402 1543 873 1759">• 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. <li data-bbox="402 1766 873 1900">• 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. | <ul style="list-style-type: none"> <li data-bbox="954 1543 1516 1682">• 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. <li data-bbox="954 1688 1516 1818">• 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. |

| Identified Shortfalls in the Risk Assessment | Shortfall Description and Corresponding Risk Element Affected: Threat (T), Vulnerability (V), Consequence (C) | Why It Matters |
|--|---|---|
| Data sources, underlying assumptions and judgments, and sources of uncertainty not always documented | <ul style="list-style-type: none"> 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. | <ul style="list-style-type: none"> 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. 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 | <ul style="list-style-type: none"> 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. | <ul style="list-style-type: none"> 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. |
| natural hazards | <ul style="list-style-type: none"> 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. | <ul style="list-style-type: none"> 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. |

| Identified Shortfalls in the Risk Assessment | Shortfall Description and Corresponding Risk Element Affected: Threat (T), Vulnerability (V), Consequence (C) | Why It Matters |
|---|--|--|
| feedback data on pipeline system performance, including cybersecurity | <ul style="list-style-type: none"> 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. | <p>V</p> <ul style="list-style-type: none"> 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. |
| physical pipeline condition | <ul style="list-style-type: none"> 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. | <p>V</p> <ul style="list-style-type: none"> 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. |

| Identified Shortfalls in the Risk Assessment | Shortfall Description and Corresponding Risk Element Affected: Threat (T), Vulnerability (V), Consequence (C) | Why It Matters |
|--|--|--|
| cross-sector interdependencies | <ul style="list-style-type: none"> 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. | <ul style="list-style-type: none"> 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

⁸⁰See 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).

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

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

⁸²See 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.

⁸³See [GAO-13-353](#).

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.

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.

⁸⁴During 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 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 CFSSR 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.

⁸⁵The 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.

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

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

⁸⁶TSA 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.

⁸⁷GAO, *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).

of effective performance.⁸⁸ Table 7 identifies each key attribute of effective performance measures along with its definition.

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 NTS, 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

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

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

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

⁹⁰Formula 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.

some core program activities,⁹¹ such as updating the 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

⁹¹For 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 timely and relevant intelligence and information to industry; and promoting pipeline security awareness in communities surrounding critical pipeline assets and systems.

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 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 implementation 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

⁹²GAO, *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).

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

⁹³For 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".

-
- 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 safeguards. 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,

⁹⁴For 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.

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

⁹⁶For 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”.

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

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

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.

⁹⁹[GAO-14-704G](#).

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

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 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.

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

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.

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 CFRs. (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

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

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 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](#).

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 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

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.

Vulnerability

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

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.

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.

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

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.

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

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 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.

increasing levels of network technologies 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.

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.

Consequence

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

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.

**Appendix II: Description of Areas for
Improvement in the Pipeline Security Branch's
Pipeline Relative Risk Ranking Tool**

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.

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

Chris P. Currie at (404) 679-1875 or curriec@gao.gov
Nick Marinos at (202) 512-9342 or marinosn@gao.gov.

Staff Acknowledgments

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.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (<https://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <https://www.gao.gov> and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).
Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <https://www.gao.gov/fraudnet/fraudnet.htm>

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800, U.S. Government Accountability Office, 441 G Street NW, Room 7149, Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707, U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548



Please Print on Recycled Paper.