United States Government Accountability Office

Testimony

Before the Subcommittee on Energy, Committee on Energy and Commerce, House of Representatives

For Release on Delivery
Expected at 10:00a.m ET
Wednesday, May 1, 2019

CRITICAL INFRASTRUCTURE PROTECTION

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

Statement of William Russell, Acting Director, Homeland Security and Justice

May 1, 2019

CRITICAL INFRASTRUCTURE PROTECTION

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

GAO Highlights

Highlights of GAO-19-542T, a testimony before the Subcommittee on Energy, Committee on Energy and Commerce, House of Representatives

Why GAO Did This Study

More than 2.7 million miles of pipeline transport and distribute natural gas, oil, 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. Pipeline system disruptions could result in commodity price increases or widespread energy shortages. Several federal and private entities have roles in pipeline security. TSA is primarily responsible for the federal oversight of pipeline physical security and cybersecurity.

This statement summarizes previous GAO findings related to TSA's management of its pipeline security program. It is based on a prior GAO product issued in December 2018, along with updates as of April 2019 on actions TSA has taken to address GAO's recommendations from the report. To conduct the prior work, 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—a non-generalizable sample selected based on volume, geography, and material transported—and representatives from five pipeline industry associations. GAO also reviewed information on TSA's actions to implement its prior recommendations.

What GAO Recommends

GAO made 10 recommendations in its December 2018 report to strengthen TSA's management of its pipeline security program. DHS agreed and has described planned actions or timeframes for addressing these recommendations.

View GAO-19-542T. For more information, contact William Russell at (202) 512-8777 or russellw@gao.gov.

What GAO Found

The Department of Homeland Security's (DHS) Transportation Security Administration (TSA) has developed and provided pipeline operators with voluntary security guidelines, and also evaluates the vulnerability of pipeline systems through security assessments. However, GAO's prior work, reported in December 2018, identified some weaknesses and made recommendations to strengthen TSA's management of key aspects of its pipeline security program.

Pipeline security guidelines. GAO reported that TSA revised its voluntary pipeline security 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 (NIST) Framework for Improving Critical Infrastructure Cybersecurity. However, TSA's revisions do not include all elements of the current NIST framework and TSA does not have a documented process for reviewing and revising its guidelines on a regular basis. GAO recommended that TSA implement a documented process for reviewing and revising TSA's *Pipeline Security Guidelines* at defined intervals. TSA has since outlined procedures for reviewing its guidelines, which GAO is reviewing to determine if they sufficiently address the recommendation.

Workforce planning. GAO reported that the number of TSA security reviews of pipeline systems has varied considerably over time. TSA officials stated that staffing limitations within its Pipeline Security Branch have prevented TSA from conducting more reviews. Staffing levels for the branch have varied significantly, ranging from 1 full-time equivalent in 2014 to 6 from fiscal years 2015 through 2018. 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. GAO recommended that TSA develop a strategic workforce plan, which TSA plans to complete by July 2019.

Pipeline risk assessments. GAO identified factors that likely limit the usefulness of TSA's risk assessment methodology for prioritizing pipeline security reviews. For example, 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. GAO recommended that TSA update its risk ranking tool to include up-to-date data to ensure it reflects industry conditions and fully document the data sources, assumptions and judgments that form the basis of the tool. As of April 2019, TSA reported taking steps to address these recommendations. GAO is reviewing documentation of these steps to determine if they sufficiently address the recommendations.

Monitoring performance. GAO reported that conducting security reviews was the primary means for TSA to assess the effectiveness ofits efforts to reduce pipeline security risks. However, TSA has not tracked the status of key security review recommendations for the past 5 years. GAO recommended that TSA take steps to update information on security review recommendations and monitor and record their status, which TSA plans to address by November 2019.

Chairman Rush, Ranking Member Upton, and Members of the Subcommittee:

Thank you for the opportunity to discuss our work on the Transportation Security Administration's (TSA) efforts to manage its pipeline security program. 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 pipelines transport and distribute the natural gas, oil, and other hazardous liquids that U.S. citizens and businesses depend on to operate vehicles and machinery, heat homes, generate electricity, and manufacture products. A minor pipeline system disruption could result in commodity price increases, while prolonged pipeline disruptions could lead to widespread energy shortages.[1] A disruption of any magnitude may affect other domestic critical infrastructure and industries that are dependent on pipeline system commodities.

The interstate pipeline system runs through both remote and highly populated urban areas, and it 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, pipeline systems are attractive targets for terrorists, hackers, foreign nations, criminal groups, and others with malicious intent.

New threats to the nation's pipeline systems have evolved to include sabotage by environmental activists and cyber-attack or intrusion by nations. For example, in October 2016 environmental activists forced the shutdown of five crude oil pipelines in four states.[2] 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

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

[2]Congressional Research Service, Pipeline Security: Recent Attacks, IN106103 (Washington, D.C.: Apr. 11, 2017).

sectors, including the energy sector, and collected information pertaining to Industrial Control Systems.[3]

TSA, within the Department of Homeland Security (DHS), has primary oversight responsibility for the physical security and cybersecurity of transmission and distribution pipeline systems.[4] TSA's Security Policy and Industry Engagement's Pipeline Security Branch is charged with managing its pipeline security program. The Pipeline Security Branch first issued its voluntary *Pipeline Security Guidelines* in 2011 and released revised guidelines in March 2018. The Pipeline Security Branch is responsible for conducting voluntary security reviews—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*. CSRs are voluntary on-site reviews of a pipeline owner's corporate policies and procedures. CFSRs are voluntary on-site inspections of critical pipeline facilities, as well as other select pipeline facilities, throughout the nation.

My testimony today summarizes findings from our December 2018 report examining TSA's management of its pipeline security program.[5] In addition, this statement contains updates from TSA as of April 2019 about actions it has taken to address the recommendations made in our December 2018 report. For this report, we reviewed and analyzed relevant documents from TSA and other federal entities, evaluated TSA pipeline risk assessment efforts, and interviewed TSA officials, including officials within TSA's Pipeline Security Branch. We also interviewed representatives from five major industry associations and security personnel from 10 pipeline operators to collect a range of perspectives on

[3]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)). Industrial control systems include software-based systems used to monitor and control many aspects of network operation for pipeline networks

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

[5]GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management*, GAO-19-48 (Washington, D.C.: Dec. 18, 2018).

topics relevant to pipeline security.[6] While the information gathered during the operator interviews cannot be generalized to all pipeline operators, it provides a range of perspectives on a variety of topics relevant to pipeline security. Additional details on the scope and methodology are available in our published report.

The work upon which this statement is based was conducted 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.

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

In our December 2018 report, we found that TSA provides pipeline operators with voluntary security guidelines that operators can implement to enhance the security of their pipeline facilities. TSA also evaluates the vulnerability of pipeline systems through security assessments. Pipeline operators and industry association representatives who we interviewed also reported exchanging risk-related security information and coordinating with federal and nonfederal entities, including TSA. However, we also identified weaknesses in several areas of TSA's pipeline security program management, including: (1) updating and clarifying pipeline security guidelines; (2) planning for workforce needs; (3) assessing pipeline risks; and (4) monitoring program performance.

Exchanging Security Information and Coordinating with Federal and Nonfederal Entities

We found in our December 2018 report that all of the pipeline operators and industry association representatives that we interviewed reported receiving security information from federal and nonfederal entities. For example, DHS components including TSA's Intelligence and Analysis and NCCIC share security-related information on physical and cyber threats and incidents. Nonfederal entities included Information Sharing and

[6]We selected the 10 pipeline operators from TSA's list of the top 100 critical pipeline systems and chose them to ensure a mixture of the following characteristics: (a) type of pipeline commodity transported (i.e. natural gas and 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.

Analysis Centers, fusion centers, industry associations, and subsector coordinating councils.[7]

Pipeline operators also reported that they share security-related information with TSA and the NCCIC. For example, TSA's *Pipeline Security Guidelines* requests that pipeline operators report physical security incidents to the Transportation Security Operations Center (TSOC) and any actual or suspected cyberattacks to the NCCIC. According to TSA officials, TSOC staff analyzes incident information for national trends and common threats, and then shares their observations with pipeline operators during monthly and quarterly conference calls.

Updating Pipeline Security Guidelines

In our December 2018 report, we found that the pipeline operators 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* that the operators determined to be applicable to their operations.[8] Five of the 10 pipeline operators 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. Pipeline operators and industry association representatives reported that their members also use the Interstate Natural Gas Association of America's Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry,[9] the American Petroleum Institute's Pipeline SCADA Security standard,[10] and the National Institute of Standards and Technology's (NIST) Cybersecurity Framework as sources of

[7]Sector coordinating councils are self-organized, self-run, and self-governed private sector councils that interact on a wide range of sector-specific strategies, policies, and activities. The 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. For example, the Pipeline Modal Sector Coordinating Council has been established to represent pipeline operators.

[8]Transportation Security Administration, *Pipeline Security Guidelines* (April 2011).

[9]Interstate 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).

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

cybersecurity standards, guidelines, and practices that may be scaled and applied to address a pipeline operator's cybersecurity risks.[11]

We found that TSA's Pipeline Security Branch had issued revised *Pipeline Security Guidelines* in March 2018, but TSA had 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 was initially issued in February 2014. However, because NIST released version 1.1 of the Cybersecurity Framework in April 2018, the guidelines that TSA released in March 2018 did not incorporate cybersecurity elements that NIST added to the latest Cybersecurity Framework, such as the Supply Chain Risk Management category.[12] Without a documented process defining how frequently TSA is to review and, if deemed necessary, revise its guidelines, TSA cannot ensure that the guidelines reflect the latest known standards and best practices of physical security and cybersecurity.

We recommended that TSA implement a documented process for reviewing, and if deemed necessary, revising TSA's *Pipeline Security Guidelines* at regular defined intervals. DHS agreed and estimated that this effort would be completed by April 30, 2019. In April 2019, TSA provided us with documentation outlining procedures for reviewing these guidelines. We are currently assessing this information to determine if it sufficiently addresses this recommendation.

We also found that TSA's *Pipeline Security Guidelines* lacked clarity in the definition of key terms used to determine critical facilities. TSA initially identifies the 100 highest risk pipeline systems based on the amount of material transported through the system. Subsequently, pipeline operators are to use criteria in the *Guidelines* to self-identify the critical

[11]NIST, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0* (Feb. 12, 2014).

[12]NIST 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."

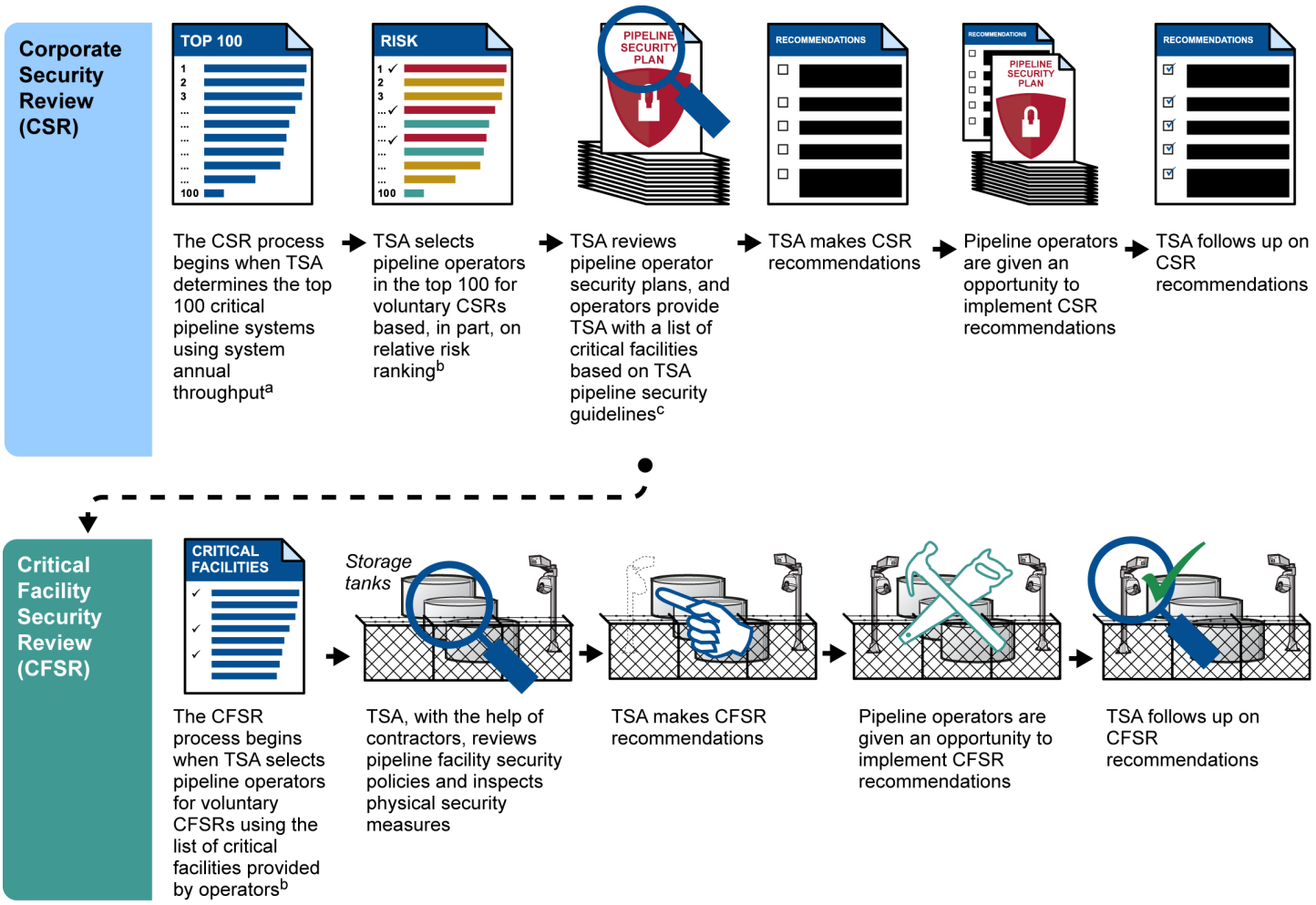
facilities within those higher risk systems and report them to TSA. TSA's Pipeline Security Branch then conducts CFSRs at the critical facilities identified by pipeline operators. However, our analysis of TSA's data found that at least 34 of the top 100 critical pipeline systems TSA deemed highest risk indicated that they had no critical facilities. Three of the 10 operators we interviewed stated that some companies that reported to TSA that they had no critical facilities may possibly be taking advantage of the guidelines' lack of clarity. For example, one of TSA's criteria for determining pipeline facility criticality states that if a facility or combination of facilities were damaged or destroyed, it would have the potential to "cause mass casualties or significant health effects." Two operators told us that individual operators may interpret TSA's criterion, "cause mass casualties or significant health effect," differently. For example, one of the 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.

Without clearly defined criteria for determining pipeline facilities' criticality, TSA cannot ensure that pipeline operators are applying guidance uniformly, that all of the critical facilities across the pipeline sector have been identified, or that their vulnerabilities have been identified and addressed. We recommended that TSA's Security Policy and Industry Engagement's Surface Division clarify TSA's *Pipeline Security Guidelines* by defining key terms within its criteria for determining critical facilities. DHS agreed and estimated that this effort would be completed by June 30, 2019.

Planning for Workforce Needs

TSA conducts pipeline security reviews—CSRs and CFSRs—to assess pipeline vulnerabilities and industry implementation of TSA's *Pipeline Security Guidelines*. However, the number of reviews conducted has varied widely from fiscal years 2014 through 2018. These reviews are intended to develop TSA's knowledge of security planning and execution at critical pipeline systems and lead to recommendations for pipeline operators to help them enhance pipeline security. For an overview of the CSR and CFSR processes, see Figure 1 below.

Figure 1: Overview of the Transportation Security Administration's (TSA) Voluntary Security Review Processes with Pipeline Operators



Source: GAO analysis of TSA information. | GAO-19-542T

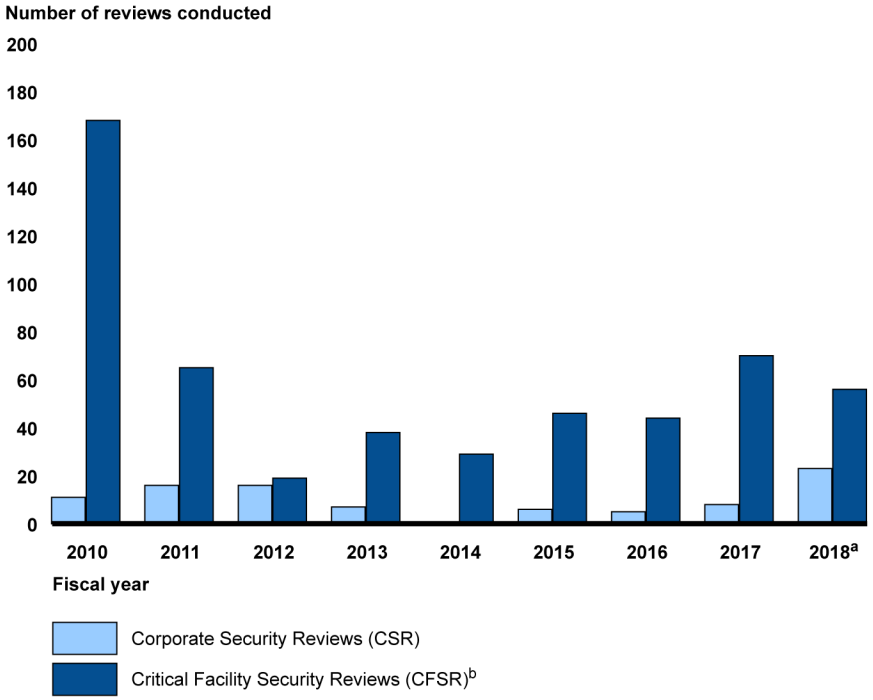
[a]TSA uses system annual throughput in determining the top 100 critical pipeline systems, which is based on the amount of hazardous liquid or natural gas product transported through a pipeline in 1 year (i.e., annual throughput measured in therms). Also, some pipeline operators own or operate more than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

[b]Because 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 as of June 2018.

[c]Under 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 .

We found that 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 (see Figure 2 below).[13] TSA officials reported that staffing limitations had prevented TSA from conducting more reviews.

Figure 2: Transportation Security Administration (TSA) Pipeline Security Reviews Conducted, Fiscal Year 2010 through Fiscal Year 2018 Year-to-Date



Source: GAO analysis of Transportation Security Administration-reported figures. | GAO-19-542T

[a]Fiscal year 2018 data are through July 31, 2018.

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

TSA Pipeline Security Branch staffing levels (excluding contractor support) also varied significantly over the past 9 years ranging from 14 full-time equivalents in fiscal years 2012 and 2013 to one in fiscal year 2014 (see Table 1 below). TSA officials stated that, while contractor

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

support has assisted with conducting CFSRs, there were no contractor personnel providing CSR support from fiscal years 2010 through 2017, but that contractors increased to two personnel in fiscal year 2018. TSA officials stated that they expected to complete 20 CSRs and 60 CFSRs per fiscal year with Pipeline Security Branch employees and contract support, and had completed 23 CSRs through July 2018 for fiscal year 2018.

Table 1: 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.

[a]TSA pipeline staffing numbers are in full-time equivalents.

In addition, pipeline operators that 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.

We found that TSA had not established a workforce plan for its Security Policy and Industry Engagement or its Pipeline Security Branch that identified staffing needs and skill sets such as the required level of cybersecurity expertise among TSA staff and contractors. We therefore recommended that TSA develop a strategic workforce plan for its Security Policy and Industry Engagement 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. DHS agreed and estimated that this effort would be completed by July 31, 2019.

Pipeline Risk Assessments

The Pipeline Security Branch has developed a risk assessment model that combines all three elements of risk—threat, vulnerability, and consequence—to generate a risk score for pipeline systems. The Pipeline Security Branch developed the Pipeline Relative Risk Ranking Tool in 2007 for use in assessing various security risks to the top 100 critical pipeline systems based on volume of material transported through the system (throughput).[14]

The risk ranking tool calculates threat, vulnerability, and consequence for each pipeline system on variables such as the amount of throughput in the pipeline system and the number of critical facilities using data collected from pipeline operators, as well as other federal agencies such as the Departments of Transportation and Defense. The ranking tool then generates a risk score for each of the 100 most critical pipeline systems and ranks them according to risk, which was information used by TSA to prioritize pipeline security assessments.

However, in our December 2018 report we found that the last time the Pipeline Security Branch calculated relative risk among the top 100 critical pipeline systems using the ranking tool was in 2014. Since the risk assessment had not changed since 2014, information on threat may be outdated and may limit the usefulness of the ranking tool in allowing the Pipeline Security Branch to effectively prioritize reviews of pipeline systems. We recommended that the Security Policy and Industry Engagement's Surface Division update the Pipeline Relative Risk Ranking Tool to include up-to-date data to ensure it reflects industry conditions, including throughput and threat data. DHS agreed and in March 2019 TSA officials reported taking steps to update the data in the Pipeline Risk Ranking Tool to reflect current pipeline industry data. We are currently reviewing those actions to determine if they sufficiently address our recommendation.

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

We also found that some of the sources of data and vulnerability assessment inputs to the ranking tool were not fully documented. For example, threats to cybersecurity were not specifically accounted for in the description of the risk assessment methodology, making it unclear if cybersecurity threats were part of the assessment's threat factor. We recommended that the Security Policy and Industry Engagement's Surface Division 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. In March 2019, TSA officials stated that they had taken steps to document this information. We are currently reviewing those steps to determine if they sufficiently address our recommendation.

Monitoring Program Performance

In our December 2018 report, we also found that TSA developed three databases to track CSR and CFSR recommendations and their implementation status by pipeline facility, system, operator, and product type. TSA officials stated that the primary means for assessing the effectiveness of the agency's efforts to reduce pipeline security risks was through conducting pipeline security reviews—CSRs and CFSRs. However, while TSA does track CFSR recommendations, we found that TSA had not tracked the status of CSR recommendations for security improvements in over 5 years—information necessary for TSA to effectively monitor pipeline operators' progress in improving their security posture. We recommended that TSA take steps to enter information on CSR recommendations and monitor and record their status. DHS agreed and estimated that this effort would be completed by November 30, 2019.

Chairman Rush, Ranking Member Upton, and Members of the Subcommittee, this completes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

GAO Contact and Staff Acknowledgments

If you or your staff members have any questions about this testimony, please contact me at (202) 512-8777 or russellw@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Other individuals making key contributions to this work include Ben Atwater, Assistant Director; Steve Komadina, Analyst-in-Charge; Nick Marinos, Michael Gilmore, Tom Lombardi, Chuck Bausell and Susan Hsu.