United States Government Accountability Office

Statement Before the Committee on Commerce, Science, and Transportation, U.S. Senate

For Release on Delivery
Expected at 10:00 a.m. ET
Tuesday, July 27, 2021

CRITICAL INFRASTRUCTURE PROTECTION

TSA Is Taking Steps to Address Some Pipeline Security Program Weaknesses

Statement of Leslie V. Gordon,
Acting Director
Homeland Security and Justice

Accessible Version

GAO@100
A Century of Non-Partisan Fact-Based Work

GAO-21-105263

GAO Highlights

Highlights of GAO-21-105263, a testimony before the Committee on Commerce, Science, and Transportation, U.S. Senate

July 27, 2021

CRITICAL INFRASTRUCTURE PROTECTION

TSA Is Taking Steps to Address Some Pipeline Security Program Weaknesses

Why GAO Did This Study

The nation's pipelines are vulnerable to cyber-based attacks due to increased reliance on computerized systems. In May 2021 malicious cyber actors deployed ransomware against Colonial Pipeline's business systems. The company subsequently disconnected certain systems that monitor and control physical pipeline functions so that they would not be compromised.

This statement discusses TSA's actions to address previous GAO findings related to weaknesses in its pipeline security program and TSA's guidance to pipeline owner/operators. It is based on prior GAO products issued in December 2018, June 2019, and March 2021, along with updates on actions TSA has taken to address GAO's recommendations as of June 2021. To conduct the prior work, GAO analyzed TSA documents; interviewed TSA officials, industry association representatives, and a sample of pipeline operators selected based on type of commodity transported and other factors; and observed TSA security reviews. GAO also reviewed TSA's May and July 2021 Pipeline Security Directives, TSA's Pipeline Security Guidelines, and three federal security alerts issued in July 2020, May 2021, and June 2021.

What GAO Recommends

In the prior reports, GAO made 15 recommendations to address pipeline security weaknesses, including clarifying its security guidelines and updating response protocols. TSA has addressed 12, and reported plans to address those remaining.

View GAO-21-105263. For more information, contact Leslie V. Gordon at (202) 512-8777 or GordonLV@gao.gov

What GAO Found

Protecting the nation's pipeline systems from security threats is a responsibility shared by both the Transportation Security Administration (TSA) and private industry stakeholders. Prior to issuing a cybersecurity directive in May 2021, TSA's efforts included issuing voluntary security guidelines and security reviews of privately owned and operated pipelines. GAO reports in 2018 and 2019 identified some weaknesses in the agency's oversight and guidance, and made 15 recommendations to address these weaknesses. TSA concurred with GAO's recommendations and has addressed most of them, such as clarifying portions of its Pipeline Security Guidelines improving its monitoring of security review performance, and assessing staffing needs.

As of June 2021, TSA had not fully addressed two pipeline cybersecurity-related weaknesses that GAO previously identified. These weaknesses correspond to three of the 15 recommendations from GAO's 2018 and 2019 reports.

- **Incomplete information for 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's risk assessment did not include information consistent with critical infrastructure risk mitigation, such as information on natural hazards and cybersecurity risks. GAO recommended that TSA develop data sources relevant to pipeline threats, vulnerabilities, and consequences of disruptions. As of June 2021, TSA had not fully addressed this recommendation.
- **Aged protocols for responding to pipeline security incidents**. GAO reported in June 2019 that TSA had not revised its 2010 Pipeline Security and Incident Recovery Protocol Plan to reflect changes in pipeline security threats, including those related to cybersecurity. GAO recommended that TSA periodically review, and update its 2010 plan. TSA has begun taking action in response to this recommendation, but has not fully addressed it, as of June 2021.

TSA's May 2021 cybersecurity directive requires that certain pipeline owner/operators assess whether their current operations are consistent with TSA's Guidelines on cybersecurity, identify any gaps and remediation measures, and report the results to TSA and others. TSA's July 2021 cybersecurity directive mandates that certain pipeline owner/operators implement cybersecurity mitigation measures; develop a Cybersecurity Contingency Response Plan in the event of an incident; and undergo an annual cybersecurity architecture design review, among other things. These recent security directives are important requirements for pipeline owner/operators because TSA's Guidelines do not include key mitigation strategies for owner/operators to reference when reviewing their cyber assets. TSA officials told GAO that a timely update to address current cyber threats is appropriate and that they anticipate updating the Guidelines over the next year.

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

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

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

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

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

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

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

protect cyber critical infrastructure as one of the four major cybersecurity challenges for the federal government.[5]

TSA, within the Department of Homeland Security (DHS), has primary oversight responsibility for the physical security and cybersecurity of transmission and distribution pipeline systems.[6] TSA's Pipeline Security Branch manages its pipeline security program. The Pipeline Security Branch first issued voluntary Pipeline Security Guidelines in 2011 and released revised guidelines in March 2018 and April 2021.[7]

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

My discussion of the actions TSA has taken to address weaknesses in its pipeline security program and the cybersecurity weaknesses that it has not fully addressed is based on two reports we issued in December 2018 and June 2019, selected updates we conducted in May 2021, and related information from our 2021 High Risk Series reports.[8] For these prior reports, we reviewed and analyzed relevant documents from TSA and other federal entities, evaluated TSA pipeline risk assessment efforts, and interviewed TSA officials, including officials within TSA's Pipeline Security Branch. We interviewed representatives from five major industry

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

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

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

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

associations and security personnel from 10 pipeline owner/operators to collect a range of perspectives on topics relevant to pipeline security.[9] While the information gathered during the operator interviews cannot be generalized to all pipeline owner/operators, it provides a range of perspectives on a variety of topics relevant to pipeline security. Additional details on the scope and methodology are available in our published reports.

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

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

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

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

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

the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Cybersecurity Threats to Pipeline Systems

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

The *2021 Annual Threat Assessment of the U.S. Intelligence Community* and the *2020 Homeland Threat Assessment*, among others, note that certain nations and criminal groups pose the greatest cyberattack threats to U.S. critical infrastructure.[14]

- **Nations of concern.** China, Russia, Iran, and North Korea have the ability to launch cyberattacks that could disrupt or damage critical infrastructure, according to the Office of the Director of National

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

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

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

Intelligence's Annual Threat Assessment. For example, China has the ability to disrupt a natural gas pipeline for days to weeks.[15]

- **Criminal groups.** In addition, according to the *2020 Homeland Threat Assessment*, cybercriminals increasingly will target critical infrastructure to generate profit using ransomware by exploiting gaps in the cybersecurity of critical infrastructure entities.

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

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

Recent events highlight the significant cyber threats facing the nation's pipeline system. According to the Colonial Pipeline Company, on May 7, 2021, the company learned that it was the victim of a cyberattack. A joint alert from CISA and the Federal Bureau of Investigation (FBI) indicated that malicious actors used DarkSide ransomware against Colonial Pipeline's information technology network.[16] The alert also explained that, to ensure the safety of the pipeline, the company disconnected certain

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

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

industrial control systems that monitor and control physical pipeline functions so that they would not be compromised by the criminals.

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

Federal Cybersecurity Challenges

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

[17]GAO-21-288.

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

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

Source: GAO analysis; images: peshkov/stock.adobe.com; Gorodenkoff/stock.adobe.com; metamorworks/stock.adobe.com; Monster Ztudio/stock.adobe.com. | GAO-21-105263

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

- Establishing a comprehensive cybersecurity strategy and performing effective oversight
  - Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.

    - Mitigate global supply chain risks (e.g., installation of malicious software or hardware).
    - Address cybersecurity workforce management challenges.
    - Ensure the security of emerging technologies (e.g., artificial intelligence and Internet of Things).
- Securing federal systems and information
    - Improve implementation of government-wide cybersecurity initiatives.
    - Address weaknesses in federal agency information security programs.
    - Enhance the federal response to cyber incidents.
- Protecting cyber critical infrastructure
    - Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks).
- Protecting privacy and sensitive data
    - Improve federal efforts to protect privacy and sensitive data.
    - Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.

Source: GAO analysis; images: peshkov/stock.adobe.com; Gorodenkoff/stock.adobe.com; metamorworks/stock.adobe.com; Monster Ztudio/stock.adobe.com. | GAO-21-105263

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

- **Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.** The White House's September 2018 National Cyber Strategy and the National Security Council's accompanying June 2019 Implementation Plan detailed the executive branch's approach to managing the nation's cybersecurity. However, in September 2020, we reported that the strategy and implementation plan addressed some, but not all, of the desirable characteristics of national strategies, such as goals and resources

needed.[18] We recommended that the National Security Council staff work with relevant federal entities to update cybersecurity strategy documents to include goals and resource information, among other things. The National Security Council staff neither agreed nor disagreed with our recommendation and has yet to address it.

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

- **Address cybersecurity workforce management challenges.** Federal and nonfederal critical infrastructure entities continue to face challenges in ensuring that their cybersecurity workforce has the appropriate skills. For example, according to a 2019 assessment from the Department of Energy, the electricity subsector continues to face challenges in recruiting and maintaining experts with strong knowledge of cybersecurity practices, as well as knowledge of industrial control systems supporting the electric grid.[20] Further, we reported in October 2020 that the Federal Aviation Administration does not currently have a staff training program specific to avionics cybersecurity and none of the agency's certification staff are required to take cybersecurity training tailored to their oversight roles.[21] Until these challenges are resolved, federal and nonfederal critical

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

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

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

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

infrastructure entities may not have the expertise necessary to address the increasing cybersecurity risks to their systems.

- **Strengthen the federal role in protecting the cybersecurity of critical infrastructure.** Since 2010, we have made nearly 80 recommendations for various federal agencies to enhance infrastructure cybersecurity. For example, in February 2020, we recommended that agencies better measure the adoption of the National Institute of Standards and Technology (NIST) framework of voluntary cyber standards and correct sector-specific weaknesses.[22] However, as of December 2020, most of these recommendations (nearly 50) have not been implemented. As a result, the risks of unprotected infrastructures being harmed are heightened.

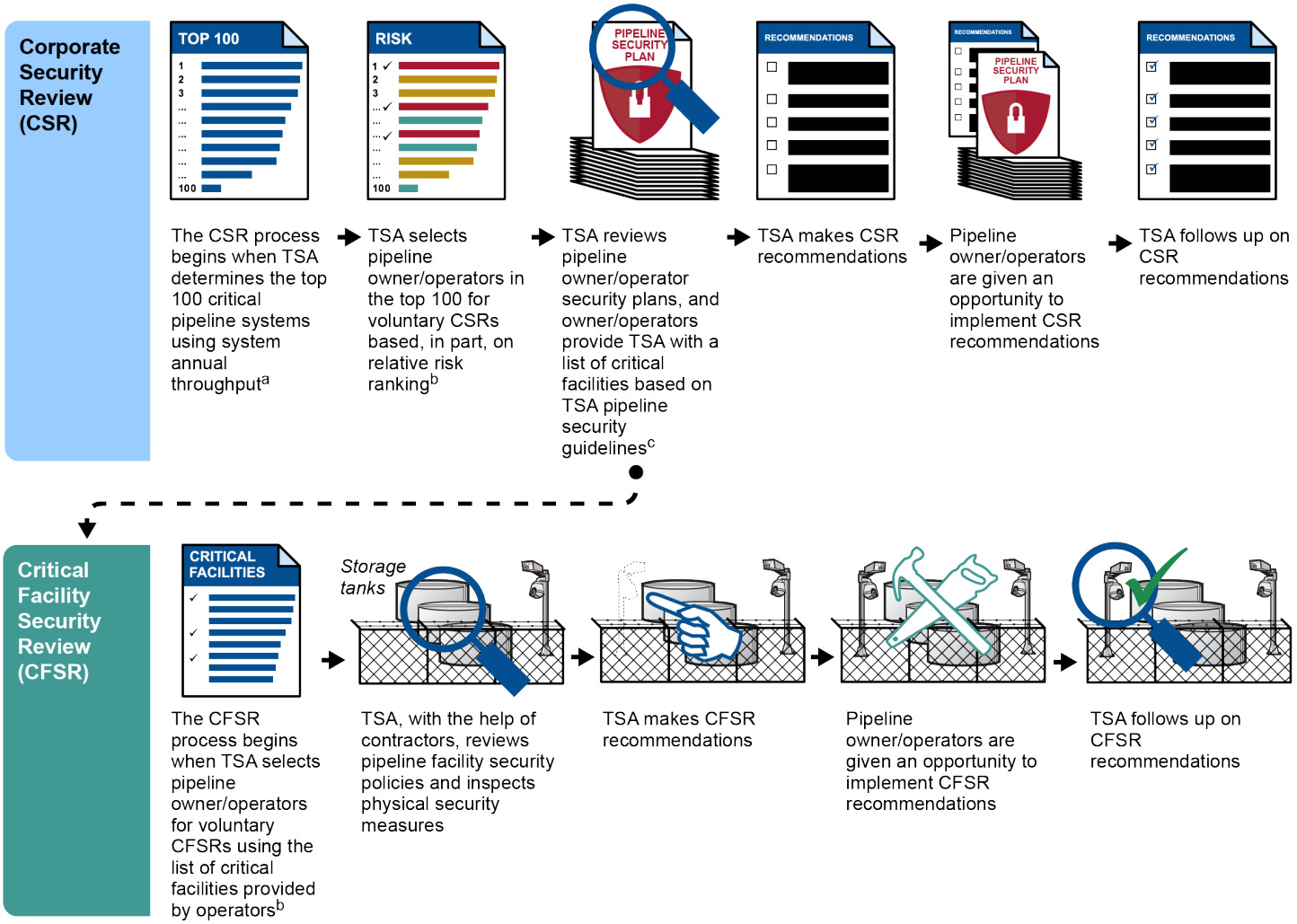
Pipeline Stakeholders' Security Roles and Responsibilities

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

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

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

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



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

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

Corporate Security Review (CSR)

- The CSR process begins when TSA determines the top 100 critical pipeline systems using system annual throughput/a/
- TSA selects pipeline owner/operators in the top 100 for voluntary CSRs based, in part, on relative risk ranking/b/

- TSA reviews pipeline owner/operator security plans, and owner/operators provide TSA with a list of critical facilities based on TSA pipeline security guidelines/c/
    - **Critical Facility Security Review (CFSR)**
        - The CFSR process begins when TSA selects pipeline owner/operators for voluntary CFSRs using the list of critical facilities provided by operators/b/
        - TSA, with the help of contractors, reviews pipeline facility security policies and inspects physical security measures
        - TSA makes CFSR recommendations
        - Pipeline owner/operators are given an opportunity to implement CFSR recommendations
        - TSA follows up on CFSR recommendations
- TSA makes CSR recommendations
- Pipeline owner/operators are given an opportunity to implement CSR recommendations
- TSA follows up on CSR recommendations

[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.

[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.

[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.

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

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

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

cybersecurity to assess cyber risks, identify any gaps, develop remediation measures, and report the results to TSA and DHS.[25]

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

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

Our December 2018 and June 2019 reports identified several weaknesses in TSA's pipeline security program and made 15 recommendations to address them (see app. I). TSA has taken actions to address several weaknesses in the management of pipeline security and has fully addressed 12 of our recommendations related to four areas. Specifically, TSA has clarified its pipeline security guidelines, improved performance monitoring, assessed staffing needs, and updated guidance on federal roles and responsibilities:

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

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

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

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

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

  TSA's Assessment Report also noted that TSA is short the necessary positions to perform the current and projected pipeline security mission, with a 41 percent increase in staffing needed to position the

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

- **Updated guidance for federal pipeline security roles.** We reported in June 2019 on the need for key pipeline security documents to reflect the current operating environment. Specifically, in 2006, TSA and the Department of Transportation's Pipeline and Hazardous Materials Safety Administration (PHMSA) signed an annex to a memorandum of understanding to further delineate their pipeline security-related responsibilities.[28] We found that the memorandum of understanding had not been reviewed to consider pipeline security developments since its inception and did not fully reflect the agencies' pipeline security and safety activities. Consequently, we recommended that the TSA and PHMSA Administrators revise the annex, to include a provision requiring periodic reviews of, and corresponding updates to, the memorandum of understanding. As of February 2020, TSA and PHMSA had addressed these recommendations by including a provision in the memorandum of understanding that committed the agencies to reviewing it at least once every 5 years.[29]

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

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

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

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

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

Incomplete Information for Pipeline Security Risk Assessments

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

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

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

and TSA uses the risk scores to prioritize its pipeline security assessments.

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

Aged Protocols for Responding to Pipeline Security Incidents

In June 2019, we reported that TSA had not reviewed or revised its 2010 Pipeline Security and Incident Recovery Protocol Plan to ensure it addressed changes in at least three key areas.[33] The 2010 plan's stated

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

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

[33]GAO-19-426.

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

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

We recommended that TSA periodically review and, as appropriate, update the 2010 Pipeline Security and Incident Recovery Protocol Plan to ensure the plan reflects relevant changes in pipeline security threats, technology, federal law and policy, and any other factors relevant to the security of the nation's pipeline systems. According to TSA officials as of May 2021, TSA completed a review of the plan and determined that

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

updates are needed and will require coordination with other agencies. Fully addressing our recommendation will better ensure that federal agencies' actions are well-coordinated in response to a pipeline-related physical or cyber incident, and that pipeline stakeholders understand federal agencies' roles and responsibilities in helping pipeline owner/operators to restore service after a pipeline-related physical or cyber incident.

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

TSA's May 2021 Directive requires certain pipeline owner/operators to take three specific actions—report cybersecurity incidents to DHS, designate a cybersecurity coordinator, and review their current activities against the Pipeline Cyber Asset Security Measures in TSA's Pipeline Security Guidelines. It directs these pipeline owner/operators to assess whether their current operations and activities to address cyber risks are consistent with the Guidelines, identify any gaps, develop remediation measures, and report the results to TSA and CISA by the end of June 2021.[35]

TSA's July 2021 Directive mandates that certain pipeline owner/operators implement cybersecurity mitigation measures; develop a cybersecurity contingency and recovery plan in the event of an incident; and undergo an annual cybersecurity architecture design review, among other things.[36] According to TSA, the July 2021 Directive was developed in consultation with CISA to include many of the cybersecurity mitigation measures noted in recent security alerts.[37]

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

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

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

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

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

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 GordonLV@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 and Kaelin Kuhn, Assistant Directors; Andrew Curry, Analyst-in-Charge; Anna Bennet, Tracey King, Susanna Kuebler, Michael Lenington, Nick Marinos, Sukhjoot Singh, and Kelsey Wilson.

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

Appendix I: Status of Selected GAO Recommendations to Strengthen Transportation Security Administration (TSA) Oversight of Pipelines

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

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

GAO recommendation	Status of recommendation and actions needed if not fully implemented
Identify or develop other data sources relevant to threat, vulnerability, and consequence consistent with the National Infrastructure Protection Plan and Department of Homeland Security (DHS) critical infrastructure risk mitigation priorities and incorporate that data into the Pipeline Relative Risk Ranking Tool to assess relative risk of critical pipeline systems, which could include data on prior attacks, natural hazards, feedback data on pipeline system performance, physical pipeline condition, and cross-sector interdependencies. (GAO-19-48)[a]	Not fully implemented. DHS stated that TSA will incorporate that data into the Pipeline Risk Ranking Tool to assess relative risk of critical pipeline systems, which could include data on prior attacks, natural hazards, feedback data on pipeline system performance, physical pipeline condition, and cross-sector interdependencies. Identifying or developing other sources relevant to threat, vulnerability, and consequence consistent with the National Infrastructure Protection Plan and DHS critical infrastructure risk mitigation priorities, and incorporating it into the risk ranking tool, would provide more assurance that TSA ranks relative risk among pipeline systems using comprehensive and accurate data.
Coordinate an independent, external peer review of TSA's Pipeline Relative Risk Ranking Tool, after the Pipeline Security Branch completes enhancements to its risk assessment approach. (GAO-19-48)[a]	Not fully implemented. DHS stated that, after completing enhancements to its risk assessment approach, TSA will take steps to coordinate an independent, external peer review of its Pipeline Relative Risk Ranking Tool. Better considering threat, vulnerability, and consequence elements in its risk assessment and incorporating an independent, external peer review in its process would provide more assurance that the Pipeline Security Branch ranks relative risk among pipeline systems using comprehensive and accurate data and methods.
Ensure that TSA has a suite of performance measures which exhibit key attributes of successful performance measures, including measurable targets, clarity, and baseline and trend data. (GAO-19-48)[a]	Recommendation implemented.
Take steps to enter information on CSR recommendations and monitor and record their status. (GAO-19-48)a	Recommendation implemented.
Improve the quality of TSA's pipeline security program data by developing written documentation of its data entry and verification procedures, implementing standardized data entry formats, and correcting existing data entry errors. (GAO-19-48)[a]	Recommendation implemented.

	GAO recommendation	Status of recommendation and actions needed if not fully implemented
Key pipeline security documents need to reflect current operating environment	Work with the Pipeline and Hazardous Materials Safety Administration (PHMSA) Administrator to develop and implement a timeline with milestone dates for reviewing and, as appropriate, updating the 2006 MOU Annex. (GAO-19-426)[b]	Recommendation implemented.[c]
	In consultation with the PHMSA Administrator, revise the 2006 MOU Annex to include a provision requiring periodic reviews of, and as appropriate, corresponding updates to the Annex. (GAO-19-426)[b]	Recommendation implemented.[c]
	Periodically review, and as appropriate, update the 2010 *Pipeline Security and Incident Recovery Protocol Plan* to ensure the plan reflects relevant changes in pipeline security threats, technology, federal law and policy, and any other factors relevant to the security of the nation's pipeline systems. (GAO-19-426)[b]	Not fully implemented. As of June 2021, TSA officials reported that they completed a review of the Pipeline Security Incident Recovery Protocol Plan and determined that updates are needed. The updates require additional coordination with PHMSA as well as internal review within TSA, according to TSA officials. By periodically reviewing and, as appropriate, updating its plan, TSA could better ensure it addresses changes in pipeline security threats and federal law and policy related to cybersecurity, incident management and DHS's terrorism alert system, among other things. TSA could also provide greater assurance that pipeline stakeholders understand federal roles and responsibilities related to pipeline incidents, including cyber incidents, and that response efforts to such incidents are well-coordinated.

Source: GAO. | GAO-21-105263

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

[b]*Critical Infrastructure Protection: Key Pipeline Security Documents Need to Reflect Current Operating Environment*, GAO-19-426 (Washington, D.C.: June 5, 2019).

[c]This recommendation was also implemented by PHMSA, in coordination with TSA.

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 our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

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 Email 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 FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

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

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