



June 2019

CRITICAL INFRASTRUCTURE PROTECTION

Key Pipeline Security Documents Need to Reflect Current Operating Environment

Accessible Version

GAO Highlights

Highlights of [GAO-19-426](#), a report to congressional committees

View [GAO-19-426](#). For more information, contact Bill Russell, (202) 512-8777, russellw@gao.gov.

Why GAO Did This Study

More than 2.7 million miles of pipeline transport natural gas, oil, and other hazardous liquids needed to operate vehicles and heat homes, among other things, in the United States.

Responsibility for safeguarding these pipelines is shared by TSA, within the Department of Homeland Security (DHS); PHMSA, within the Department of Transportation (DOT); and pipeline operators. TSA oversees the security of all transportation modes, including pipelines. PHMSA oversees pipeline safety. DHS and DOT signed a MOU on their roles across all transportation modes in 2004. In 2006, TSA and PHMSA signed an annex to the MOU (MOU Annex) to further delineate their pipeline security-related responsibilities.

The TSA Modernization Act includes a provision for GAO to review DHS and DOT roles and responsibilities for pipeline security. This report addresses, among other things: (1) the extent the MOU Annex delineates TSA's and PHMSA's pipeline security roles and responsibilities; and (2) the extent TSA has communicated federal incident response procedures for pipeline breaches to stakeholders. GAO reviewed the MOU annex and related documents and TSA's Pipeline Security and Incident Recovery Protocol Plan, and interviewed officials from PHMSA, TSA, and four pipeline associations.

What GAO Recommends

GAO is making five recommendations, including that: (1) TSA and PHMSA develop and implement a timeline for reviewing and, as appropriate, updating the 2006 MOU Annex; and (2) TSA periodically review, and as appropriate, update its 2010 pipeline incident recovery plan. DHS and DOT concurred with these recommendations.

June 2019

CRITICAL INFRASTRUCTURE PROTECTION

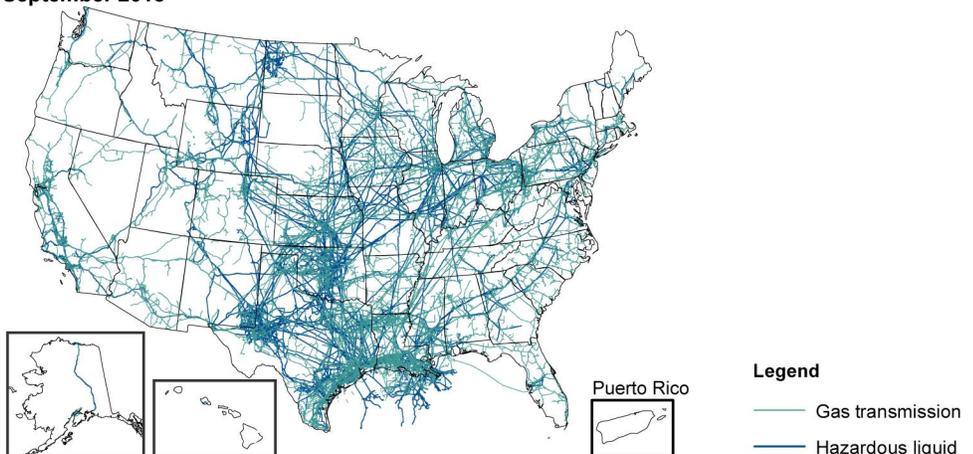
Key Pipeline Security Documents Need to Reflect Current Operating Environment

What GAO Found

The memorandum of understanding (MOU) Annex signed by the Transportation Security Administration (TSA) and Pipeline and Hazardous Materials Safety Administration (PHMSA) in 2006 delineates their mutually agreed-upon roles and responsibilities for pipeline security, but has not been reviewed to consider pipeline security developments since its inception. As a result, the annex may not fully reflect the agencies' pipeline security and safety-related activities. Efforts to update the annex were delayed by other priorities. As of June 2019, there are no timeframes for completion. By developing and implementing timeframes for reviewing the MOU Annex and updating it, as appropriate, TSA and PHMSA could better ensure any future changes to their respective roles and responsibilities are clearly delineated and updated on a regular basis.

TSA's Pipeline Security and Incident Recovery Protocol Plan, issued in March 2010, defines the roles and responsibilities of federal agencies and the private sector, among others, related to pipeline security incidents. For example, in response to a pipeline incident, TSA coordinates information sharing between federal and pipeline stakeholders and PHMSA coordinates federal activities with an affected pipeline operator to restore service. However, TSA has not revised the plan to reflect changes in at least three key areas: pipeline security threats, such as those related to cybersecurity, incident management policies, and DHS's terrorism alert system. 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.

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



Source: U.S. Department of Transportation. | GAO-19-426

Contents

Letter	1
GAO Highlights	2
Why GAO Did This Study	2
What GAO Recommends	2
What GAO Found	2
Letter	1
Background	5
MOU Annex Delineates Pipeline Security Roles and Responsibilities But Has Not Been Reviewed to Consider Pipeline Security Developments Since 2006	13
TSA and PHMSA Communicate Their Roles through Guidelines and Other Methods, and Selected Industry Stakeholders Reported the Agencies' Roles Are Clear	17
TSA Communicated Pipeline Incident Response Protocols in Its 2010 Plan, but Has Not Updated the Plan to Address Changes in Key Areas	20
Conclusions	28
Recommendations for Executive Action	29
Agency Comments and Our Evaluation	29
Appendix I: 2006 Memorandum of Understanding (MOU) Program Areas and Accompanying Text	32
Appendix II: Summary of Key Federal Agencies' and Pipeline Operator's Roles and Responsibilities	35
Appendix III: Comments from the Department of Homeland Security	39
Text of Appendix III: Comments from the Department of Homeland Security	42
Appendix IV: Comments from the Department of Transportation	45
Text of Appendix IV: Comments from the Department of Transportation	48

Appendix V: GAO Contact and Staff Acknowledgments	50
GAO Contact	50
Staff Acknowledgments	50

Table	
Table 1: 2006 MOU Program Areas and Accompanying Text	32

Figures	
Figure 1: Map of Hazardous Liquid and Natural Gas Transmission Pipelines in the United States, September 2018	6
Figure 2: Notable Pipeline Accidents in the United States from September 2010 through June 2019	8
Figure 3: Sixteen Critical Infrastructure Sectors and the Related Sector-Specific Agencies	10

Abbreviations

API	American Petroleum Institute
CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
DOE	Department of Energy
DOT	Department of Transportation
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
HSPD	Homeland Security Presidential Directive
MOU	Memorandum of Understanding
NCIRP	National Cyber Incident Response Plan
NCCIC	National Cybersecurity and Communications Integration Center
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology

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.

NRF	National Response Framework
NTAS	National Terrorism Advisory System
NTSB	National Transportation Safety Board
PHMSA	Pipeline and Hazardous Materials Safety Administration
PPD	Presidential Policy Directive
SCADA	Supervisory Control and Data Acquisition
SCC	Sector Coordinating Council
TSA	Transportation Security Administration
TSOC	Transportation Security Operations Center



June 5, 2019

The Honorable Roger Wicker
Chairman
The Honorable Maria Cantwell
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Bennie G. Thompson
Chairman
The Honorable Mike Rogers
Ranking Member
Committee on Homeland Security
House of Representatives

The Honorable Peter A. DeFazio
Chairman
The Honorable Sam Graves
Ranking Member
Committee on Transportation and Infrastructure
House of Representatives

More than 2.7 million miles of pipeline 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. The interstate pipeline system runs through remote, as well as highly populated urban areas, and is generally considered to be resilient and versatile. However, it is also vulnerable to accidents, operating errors, and malicious physical attack. Some pipelines are also vulnerable to aging infrastructure. In addition, pipelines increasingly rely on sophisticated networked computerized systems and electronic data, which are vulnerable to cyber attack or intrusion.

Many pipelines transport volatile, flammable, or toxic products. As demonstrated by the September 2018 explosion of a Merrimack Valley, Massachusetts natural gas distribution pipeline system, the potential consequences of a catastrophic event on life, property, the economy, and the environment resulting from a natural disaster, operational accident, or

from a successful physical or cyber attack on a pipeline are high.¹ A minor pipeline system disruption could result in commodity price increases while prolonged pipeline disruptions could lead to widespread energy shortages.² Further, disruption of any magnitude may affect other domestic critical infrastructure and industries that are dependent on pipeline system commodities.

Responsibility for safeguarding the nation's pipeline systems from such catastrophic events is shared by the Department of Homeland Security's (DHS) Transportation Security Administration (TSA), the Department of Transportation's (DOT) Pipeline and Hazardous Materials Safety Administration (PHMSA), and pipeline owners and operators. TSA is responsible for security in all modes of transportation, which includes the physical security and cybersecurity of the nation's pipeline system. PHMSA is responsible for overseeing the safety of the nation's pipeline system. In September 2004, DHS and DOT entered into a memorandum of understanding (MOU) regarding their respective roles across all modes of transportation. In August 2006, TSA and PHMSA signed an Annex to the MOU (MOU Annex) to further delineate lines of authority and responsibility between the agencies on pipeline and hazardous materials transportation security. The MOU Annex recognizes TSA as the lead federal entity for transportation security, including hazardous materials and pipeline security, and PHMSA as responsible for administering a national program of safety in natural gas and hazardous liquid pipeline transportation, including identifying pipeline safety concerns and developing uniform safety standards. Private sector pipeline operators are responsible for implementing asset-specific safety standards and protective security measures.

In September 2018, we issued an update to the information security high-risk area that identified actions needed to address cybersecurity

¹According to the National Transportation Safety Board, a series of explosions and fires occurred on September 13, 2018, after high-pressure natural gas was released into a low-pressure gas distribution system in the Merrimack Valley, Massachusetts. The system overpressure damaged 131 structures, and destroyed at least five homes in the city of Lawrence and the towns of Andover and North Andover. One person was killed and at least 21 individuals, including 2 firefighters, were transported to the hospital. The incident is not believed to be the result of an intentional act, such as terrorist or cyber attack. According to PHMSA, this incident could not have resulted from a cyber attack because of the age and lack of connectivity of the infrastructure involved.

²Transportation Security Administration, *Biennial National Strategy for Transportation Security: Report to Congress* (Washington, D.C.: Apr. 4, 2018).

challenges facing the nation.³ For example, challenges we identified included protecting the cybersecurity of the nation's critical infrastructure, which includes pipeline systems. We last reported on pipeline security in December 2018. TSA concurred with all ten of our recommendations, and we will continue to monitor the status of implementation.⁴

The TSA Modernization Act includes a provision for us to conduct a study regarding the roles and responsibilities of DHS and the DOT for pipeline security.⁵ We briefed your offices on our preliminary results on March 29, 2018. This report addresses the following questions: (1) To what extent does the 2006 Annex to the MOU between DHS and DOT delineate TSA's and PHMSA's responsibilities for pipeline security? (2) How do TSA and PHMSA communicate their roles and responsibilities related to pipeline safety and security and what are industry stakeholder views on the clarity of the communication? (3) To what extent has federal incident response processes and procedures for pipeline security breaches been communicated to stakeholders?

To identify the extent to which the 2006 Annex to the MOU between DHS and DOT delineates TSA and PHMSA responsibilities for pipeline security, we reviewed relevant TSA and PHMSA documents including the 2006 MOU Annex, action plans for implementing provisions of the MOU Annex, and documents related to the agencies' process for revising the

³GAO, *High Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, [GAO-18-622](#) (Washington, D.C.: Sept. 6, 2018).

⁴Among other things, we recommended TSA implement a documented process for reviewing, and if necessary, for revising TSA's Pipeline Security Guidelines at regular defined intervals; define key terms within its criteria for determining critical facilities; update the Pipeline Relative Risk Ranking Tool to ensure it reflects industry conditions, including throughput and threat data; and identify or develop other data sources relevant to threat, vulnerability, and consequence consistent and incorporate that data into the Pipeline Relative Risk Ranking Tool. See 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).

⁵The TSA Modernization Act, enacted as division K of the FAA Reauthorization Act of 2018, further provides that our study should address, among other things, whether, and if so how, pipeline sector stakeholders share security-related information, the guidance pipeline operators report using to address security risks, the extent to which TSA ensures its guidelines reflect the current threat environment, the extent to which TSA has assessed security risks to pipeline systems, and the extent to which TSA has assessed its effectiveness in reducing pipeline security risks. See Pub. L. No. 115-254, div. K, tit. I, subtit. G, § 1980, 132 Stat. 3186 (2018). [GAO-19-48](#) addressed these provisions of the law.

Annex. We assessed TSA and PHMSA efforts to revise the 2006 MOU Annex against relevant standards in the *Standards for Internal Controls in the Federal Government* and project management guidance related to periodically reviewing policies and developing project timelines with milestone dates.⁶ We also reviewed relevant laws, regulations, and statements of Executive Branch policy, including presidential directives. In addition, we conducted semi-structured interviews with TSA and PHMSA officials to obtain their perspectives on respective pipeline security roles and responsibilities.

To identify how TSA and PHMSA communicate their roles and responsibilities related to pipeline safety and security, we reviewed TSA and PHMSA documents that describe each agency's respective pipeline security and safety programs such as TSA's Pipeline Security Guidelines, and PHMSA's pipeline safety regulations and advisory bulletins. We conducted interviews with TSA and PHMSA officials to identify the types of activities they conduct to communicate and clarify their respective roles and responsibilities to stakeholders. To assess industry stakeholder views on the clarity of the communication, we interviewed representatives of the four of the five major associations with ties to the pipeline industry.⁷

To identify the extent to which federal incident response processes and procedures for pipeline security breaches have been communicated to stakeholders, we reviewed TSA's *Pipeline Security and Incident Recovery Protocol Plan* against criteria outlined in the *Standards for Internal Control in the Federal Government* related to periodic review of policies, procedures, and related control activities. To determine the extent that the plan remains current and reflects relevant federal laws and policies, we reviewed federal laws related to critical infrastructure protection that had been enacted since TSA issued the plan in March 2010, and federal incident management policies referenced by the plan including, the Federal Emergency Management Agency's (FEMA) National Response Framework (NRF) and National Incident Management System (NIMS). We also interviewed TSA, PHMSA, and association officials to gather

⁶GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: September 2014) and Project Management Institute, Inc. *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*, Sixth Edition, 2017. PMBOK is a trademark of Project Management Institute, Inc.

⁷We did not meet with the Association of Oil Pipe Lines representatives because they declined our request for interview.

their perspectives on pipeline incident response processes and procedures for responding to pipeline security breaches.

For each objective, we interviewed representatives of four of five major associations with ties to the pipeline industry: the American Petroleum Institute (API), the American Gas Association, the Interstate Natural Gas Association of America, and the American Public Gas Association. While the information gathered during association interviews cannot be generalized to all pipeline operators, it provides a range of perspectives on a variety of topics relevant to the 2006 MOU Annex.

We conducted this performance audit from January to June 2019 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

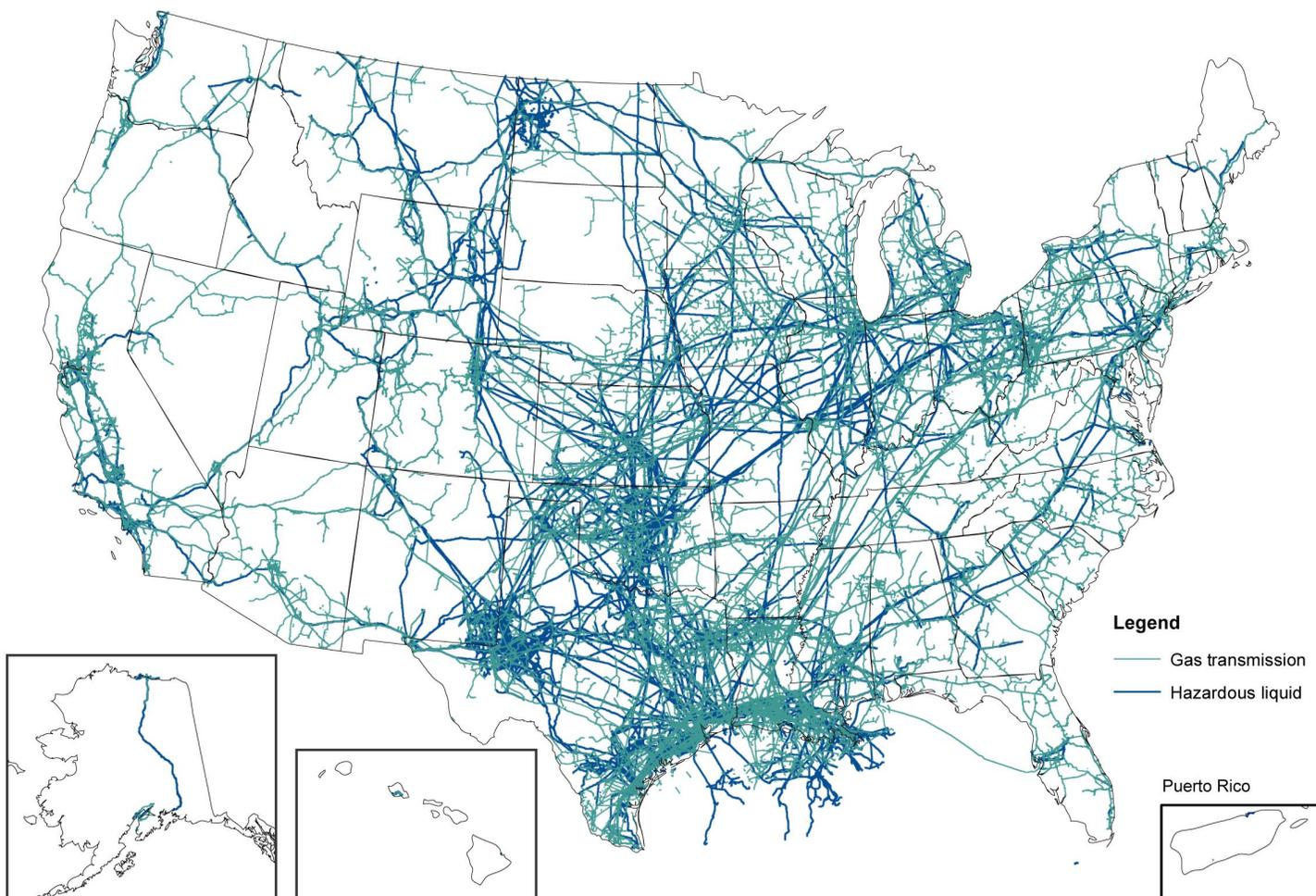
Overview of U.S. Pipeline System

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

- 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-19-426

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 through automated industrial control systems or Supervisory Control and Data Acquisition (SCADA) systems using remote sensors, signals, and preprogrammed parameters to activate and

deactivate valves and pumps to maintain flows within established tolerance levels.⁸

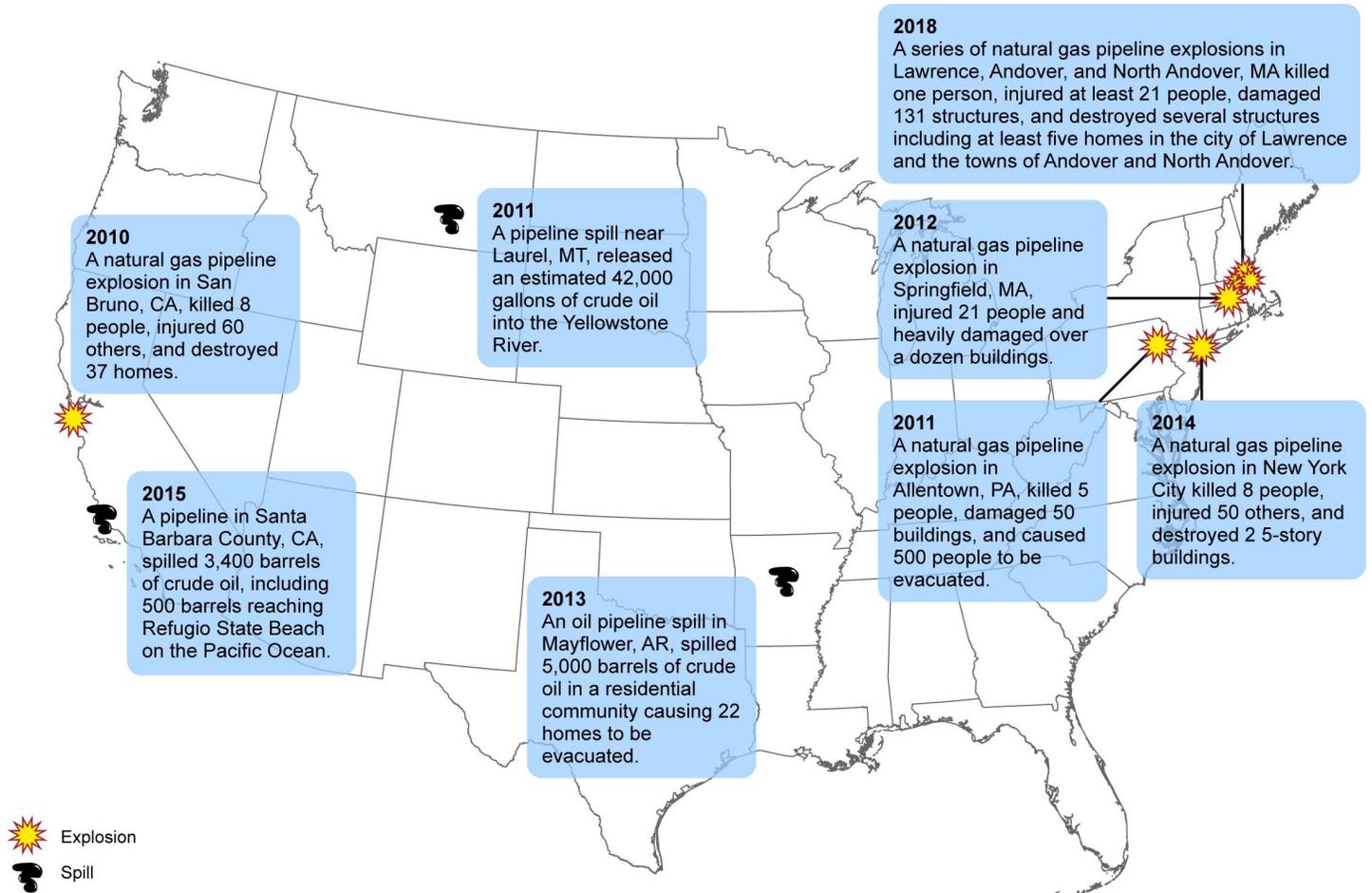
Threats to Pipeline Safety and Security

Pipeline accidents can occur from a variety of causes, including third-party excavation, corrosion, mechanical failure, control system failure, and operator error. Natural forces, such as floods and earthquakes, can also damage pipelines. Although pipeline releases have caused relatively few fatalities, a single pipeline accident can be catastrophic in terms of public safety and environmental damage.⁹ Figure 2 shows notable pipeline accidents since September 2010.

⁸SCADA is a computer-based system, which is a computer-based system used by industries and critical infrastructure to monitor and control sensitive processes and physical functions. Control systems can be used to monitor simple processes—for example, the environmental conditions in a small office building—or to manage the more complex activities of a municipal water system or nuclear power plant. Control systems are vulnerable to cyber-attack from inside or outside the control system network.

⁹Releases from pipelines have caused relatively few annual injuries or fatalities compared to other product transportation modes. See Bureau of Transportation Statistics, *Table 2-2: Injured Persons by Transportation Mode*, accessed Apr. 12, 2019, <https://www.bts.gov/content/injured-persons-transportation-mode>; and *Table 2-4: Distribution of Transportation Fatalities by Mode*, accessed Apr. 12, 2019, <https://www.bts.gov/content/distribution-transportation-fatalities-mode>.

Figure 2: Notable Pipeline Accidents in the United States from September 2010 through June 2019



Source: Congressional Research Service; National Transportation Safety Board; Map Resources (map). | GAO-19-426

According to TSA, pipelines are also vulnerable to physical attacks by crude or unsophisticated tactics, such as rudimentary explosives, arson, or equipment sabotage—largely due to their stationary nature, the volatility of transported products, and the dispersed nature of pipeline networks spanning urban and outlying areas. Threats to the nation’s pipeline systems include sabotage by activists, physical attack by terrorists, and cyber attack or intrusion by nations.¹⁰ In October 2016, environmental activists forced the shutdown of five crude oil pipelines in

¹⁰Nations, including nation-state, state-sponsored, and state-sanctioned programs, use cyber tools as part of their information-gathering and espionage activities.

four states: Minnesota, North Dakota, Montana, and Washington State. Further, in January 2019, the Director of National Intelligence stated that China has the ability to launch cyber attacks that have caused localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States.¹¹

Key Critical Infrastructure Protection Guidance and Presidential Directives

Federal policy and public-private plans establish the roles and responsibilities for the protection of critical infrastructure, including pipelines. These policies and public private plans include Presidential Policy Directive /PPD-21 (PPD-21) and the National Infrastructure Protection Plan (NIPP). PPD-21, issued in February 2013, was developed to advance a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure, which includes pipelines.¹² PPD-21 reflects an all-hazards approach to protecting critical infrastructure, by accounting for the protection of critical infrastructure from natural or manmade threats or incidents.¹³ Examples of threats or incidents include natural disasters, cyber incidents, industrial accidents, pandemics, acts of terrorism, sabotage, and destructive criminal activity targeting critical infrastructure. PPD-21 also identifies the 16 critical infrastructure sectors and assigns roles and responsibilities for each sector among nine designated federal sector-specific agencies as shown in Figure 3.

¹¹Congressional Research Service, *Pipeline Security: Homeland Security Issues in the 116 Congress*, IN11060 (Washington, D.C.: March 1, 2019).

¹²White House, *Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 12, 2013). PPD-21 revoked Homeland Security Presidential Directive/HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection*, issued December 17, 2003, but provided that plans developed pursuant to HSPD-7 shall remain in effect until specifically revoked or superseded.

¹³PPD-21 defines the term “all hazards” to mean 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.

Figure 3: Sixteen Critical Infrastructure Sectors and the Related Sector-Specific Agencies



Sector-specific agency

Departments of Agriculture (USDA), Defense (DOD), Energy (DOE), Health and Human Services (HHS), Homeland Security (DHS), Transportation (DOT), the Treasury; Environmental Protection Agency (EPA); and the General Services Administration (GSA)

Source: GAO analysis of Presidential Policy Directive/PPD-21 and DHS's National Infrastructure Protection Plan 2013; Art Explosion (clip art). | GAO-19-426

While PPD-21 identifies the critical infrastructure sectors and assigns responsibility for each sector's sector-specific agency, the NIPP outlines critical infrastructure stakeholder roles and responsibilities regarding critical security and resilience. The NIPP 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. For example, DHS and DOT are designated as co-sector-specific agencies for the transportation systems sector, which includes pipelines. Each sector also has a government coordinating council,¹⁴ 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.¹⁵ For example, the Transportation Government Coordinating Council has been established, and the Pipeline Modal SCC has also been established to represent pipeline operators.

Pipeline Stakeholder 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 safety and security.¹⁶ The entities primarily responsible for pipeline safety and security are included below.

Transportation Security Administration (TSA). TSA has primary oversight responsibility for the physical security and cybersecurity of transmission and distribution pipeline systems.¹⁷ Within TSA, the Policy, Plans, and Engagement's Pipeline Security Branch is charged with overseeing its pipeline security program. Pursuant to the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act), TSA's Pipeline Security Branch issued voluntary

¹⁴Government 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.

¹⁵SCCs are self-organized, self-run, and self-governed private sector councils that interact on a wide range of sector-specific strategies, policies, and activities.

¹⁶Federal agencies that also have roles in overseeing aspects of pipeline safety and security include the Department of Energy (DOE), the Federal Energy Regulatory Commission (FERC), and, within DHS, the Cybersecurity and Infrastructure Security Agency (CISA).

¹⁷See Pub. L. No. 107-71, 115 Stat.597 (2001); 49 U.S.C. § 114(d).

Pipeline Security Guidelines in 2011, and released revised guidelines in March 2018.¹⁸ Further, in accordance with the 9/11 Commission Act, TSA's Pipeline Security Branch also identifies the top 100 critical pipeline systems in the nation.¹⁹ TSA also ranks the relative risk among these top 100 systems. Additionally, the Pipeline Security Branch is responsible for conducting voluntary security reviews, which assess the extent to which these 100 pipeline systems are following the intent of TSA's Pipeline Security Guidelines.²⁰

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 may relate to pipeline security.²¹ PHMSA develops regulations for domestic interstate and intrastate natural gas and hazardous liquid pipelines. Its regulatory programs are focused on ensuring safety in the design, construction, operation, and maintenance of pipelines. Under PHMSA's pipeline safety program, pipeline operators have primary responsibility for ensuring the integrity of their pipelines. PHMSA and some state pipeline safety offices are responsible for conducting inspections to oversee operators' compliance with federal pipeline safety regulations and other federal requirements.²² Inspectors from PHMSA's

¹⁸See Pub. L. No. 110-53, § 1557(d), 121 Stat. 266, 475-76 (2007); 6 U.S.C. § 1207(d).

¹⁹See 6 U.S.C. § 1207(b).

²⁰These voluntary security reviews include corporate security reviews, which consist of on-site reviews of a pipeline owner's corporate policies and procedures. TSA also conducts critical facility security reviews, which are on-site reviews of critical and other pipeline facilities throughout the nation. TSA requests selected operators to participate in these reviews. Operators can decline to participate; however, according to TSA officials, no operator has declined to participate in either type of review since TSA began the programs in 2003 and 2008 respectively.

²¹The 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). While primary responsibility for pipeline security transferred with TSA to DHS, primary responsibility for regulating the safety of hazardous materials transportation via pipeline and the safety of pipeline systems remained with DOT. See 49 U.S.C. § 108; 49 C.F.R. pts. 190-199.

²²Under federal pipeline safety laws, states may assume inspection and enforcement responsibilities for intrastate gas and hazardous liquid pipelines, which are primarily natural gas distribution pipelines. See 49 U.S.C. § 108; 49 C.F.R. pts. 190-199; 49 U.S.C. §§ 60105-60106, 60108.

five regional offices and states are responsible for inspecting nearly 3,000 companies that operate 2.7 million miles of pipelines.

Private sector. Although TSA has primary federal responsibility for overseeing interstate pipeline security, private sector and publicly-owned pipeline operators are responsible for implementing asset-specific protective security measures. As we previously reported, since the September 11th terrorists attacks, operators have increased their attention on security by incorporating security practices and programs into their overall business operations.²³ Pipeline operators' interests and concerns are primarily represented by five major trade associations—the Interstate Natural Gas Association of America, American Gas Association, 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.

MOU Annex Delineates Pipeline Security Roles and Responsibilities But Has Not Been Reviewed to Consider Pipeline Security Developments Since 2006

MOU Annex Delineates Pipeline Security and Safety Roles and Responsibilities

The MOU Annex delineates TSA and PHMSA mutually agreed-upon pipeline security roles and responsibilities, consistent with their respective missions, and acknowledges that both agencies benefit by sharing each other's expertise, among other things.²⁴ Specifically, the MOU Annex identifies 11 program areas, where TSA and PHMSA agreed to

²³GAO, *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) and [GAO-19-48](#).

²⁴An accompanying action plan developed pursuant to the MOU Annex contains additional TSA and PHMSA pipeline security roles and responsibilities but TSA and PHMSA officials stated that it has not been updated since 2009 and is no longer in use.

coordinate their respective roles and responsibilities. The first program area for example, calls for both agencies to coordinate efforts to identify critical infrastructure, and to share relevant data and observations found during respective safety inspections and security assessments. Another program area addresses coordination in developing transportation security standards, regulations, guidelines, or directives. The MOU Annex further provides that TSA and PHMSA are to seek early and frequent coordination in developing such standards, regulations, guidelines, or directives. They are also to review the adequacy of existing standards in the private and public sector, and identify any gaps that should be addressed through rulemaking, guidelines, or directives, among other items. For a complete listing of the MOU Annex's 11 program areas, including TSA and PHMSA roles and responsibilities and agreed-upon actions, see appendix I.

TSA and PHMSA Do Not Have Timeframes for Reviewing the MOU Annex to Assess Pipeline Security Roles and Responsibilities

TSA and PHMSA have both noted various developments that have occurred since 2006 that may affect their roles and responsibilities related to pipeline security. However, the MOU Annex has not been updated since its inception in 2006 to consider incorporating these changes which includes subsequently issued presidential directives, the establishment of the Cybersecurity Infrastructure and Security Agency (CISA), and distinctions between current TSA and PHMSA current inspection operations. As a result, the Annex is not current and may not fully reflect the agencies' pipeline safety and security-related activities. For example, Homeland Security Presidential Directive/HSPD-7 (HSPD-7), which is cited as an underlying authority in both the 2004 MOU and 2006 MOU Annex was revoked and replaced by PPD-21 in 2013.²⁵ According to PPD-21, the directive advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure by, among other things, refining and clarifying critical infrastructure-related functions, roles, and responsibilities across the federal government. PPD-21 further provides, however, that plans developed pursuant to HSPD-7

²⁵Homeland Security Presidential Directive/HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection (Dec. 17, 2003), established a national policy for federal departments and agencies to identify and prioritize critical infrastructure and key resources and to protect them from terrorist attacks.

shall remain in effect until specifically revoked or superseded. According to TSA and PHMSA officials, statements of Executive Branch policy including presidential directives such as PPD-21 include changes that could impact their pipeline security and safety roles and should be considered in any future revisions to the MOU Annex.

Further, PHMSA officials also told us that TSA and PHMSA's roles and responsibilities in identifying critical infrastructure should be reviewed given the establishment of the CISA in November 2018. CISA, formerly the DHS National Protection and Programs Directorate, is responsible for, among other things, coordinating a national effort to secure and protect against critical infrastructure risks.²⁶ These responsibilities include coordinating with sector-specific agencies to carry out its cybersecurity and critical infrastructure activities. TSA and PHMSA officials stated that they have closely coordinated in identifying critical infrastructure when responding to past national emergencies. For example, TSA identified and provided PHMSA with information on the pipelines that supplied fuel to specific airports during the hurricane seasons in 2017 and 2018.²⁷ However, PHMSA officials stated that both TSA and PHMSA should consider reviewing how these types of efforts may need to be coordinated with CISA in the future and whether any adjustments to respective roles and responsibilities in the MOU Annex are needed. In addition, representatives from all of the industry associations that we interviewed stated that the agreement should be revised to consider how the establishment of CISA may impact current TSA and PHMSA pipeline security roles and responsibilities. TSA officials stated that they do not believe that the establishment of CISA impacts TSA's roles and responsibilities for identifying pipeline critical infrastructure. While CISA may or may not have impacts on TSA and PHMSA's pipeline security roles, reviewing the MOU Annex in light of new developments, such as

²⁶The Cybersecurity and Infrastructure Security Agency Act of 2018, enacted November 16, 2018, amended the Homeland Security Act of 2002 by, among other things, redesignating the DHS National Protection and Programs Directorate as the Cybersecurity and Infrastructure Security Agency (CISA) with responsibility for, among other things, leading cybersecurity and critical infrastructure security programs, operations, and associated policy for CISA, including national cybersecurity asset response activities, and coordinating with federal entities, including sector-specific agencies and non-federal entities to carry out the cybersecurity and critical infrastructure activities of CISA. See Pub. L. No. 115-278, 132 Stat. 4168 (2018); 6 U.S.C. § 652.

²⁷TSA identified these airports as being category X, which, in general, are the nation's largest and busiest airports as measured by the volume of passenger traffic and are potentially attractive targets for criminal and terrorist activity.

the CISA, would allow the TSA and PHMSA to determine whether updates are necessary.

TSA and PHMSA officials stated that distinctions in current inspections and enforcement operations necessitate a revision to the MOU Annex. The MOU Annex states that agencies are to explore opportunities for collaboration in inspection and enforcement activities. According to TSA and PHMSA officials, they have since explored the possibility for conducting joint activities and found that distinctions in their respective operating environments and roles and responsibilities do not allow for joint inspection and enforcement activities. For example, PHMSA conducts physical inspections of facilities to assess pipeline operators' compliance with pipeline safety regulatory requirements and relies on a range of enforcement activities, such as civil penalties to ensure that pipeline operators correct safety violations and prevent safety problems. TSA, however, conducts voluntary security assessments of pipeline's corporate security programs and critical facilities and relies on pipeline operators' willingness to participate and implement recommended changes to improve pipeline security. As a result, TSA and PHMSA officials stated that pipeline operators are reluctant to participate in a voluntary assessment that might include PHMSA inspectors because they represent a regulatory agency. TSA, PHMSA and industry association representatives we interviewed agreed that the annex should be updated to accurately reflect current distinctions in the agencies' roles and responsibilities and their respective operating environments.

PHMSA officials stated that they had planned to review the MOU Annex in 2018 to assess current roles and responsibilities and determine whether any updates to the MOU Annex were needed, but efforts were delayed because of competing priorities such as addressing the aftermath of major hurricanes in 2017 and 2018. Specifically, TSA and PHMSA had agreed to an initial list of timeframes for reviewing the MOU Annex and these timeframes called for the agencies to complete the MOU Annex revision in 2018. However, as of March 2019, TSA and PHMSA have yet to complete the review and although both agencies stated that the review is ongoing, neither agency could provide updated timeframes for completion. Furthermore, while the Annex recognizes that TSA and PHMSA may propose agreed-upon amendments or modifications to the agreement, it does not call for regular or periodic reviews to identify whether any updates or revisions are needed and, as appropriate, implemented.

TSA and PHMSA officials, as well as the industry association representatives we interviewed all reported that the MOU Annex helped to coordinate pipeline security and safety efforts because: (1) it is a signed written agreement that can be readily consulted; (2) it memorialized respective TSA and PHMSA roles and responsibilities for government leaders and staff at the time; and (3) it can be modified or amended as needed.

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. In addition, documentation of any changes made as a result of such reviews, such as changes to an entity's roles and responsibilities or in technology, should occur to ensure that such controls are clear over time as staff change within an organization. Standards for project management state that managing a project involves, among other things, developing a timeline with milestone dates to identify points throughout the project to reassess efforts under way to determine whether project changes are necessary.²⁸ By developing and implementing mutually agreed upon time frames for reviewing the annex and updating it, as appropriate, TSA and PHMSA could better ensure that the roles and responsibilities for TSA and PHMSA remain current. Additionally, including a provision in the annex for periodically reviewing for needed updates would help ensure the agreement consistently reflects relevant and updated information on TSA and PHMSA's roles and responsibilities.

TSA and PHMSA Communicate Their Roles through Guidelines and Other Methods, and Selected Industry Stakeholders Reported the Agencies' Roles Are Clear

TSA and PHMSA have communicated their respective pipeline safety and security roles and responsibilities by issuing pipeline security guidance and safety regulations, issuing a joint advisory bulletin, and maintaining

²⁸Project Management Institute, Inc. *A Guide to the Project Management Body of Knowledge* (PMBOK® Guide), Sixth Edition, 2017.

informal contacts with pipeline stakeholders when conducting outreach activities, pipeline security assessments, or safety inspections.

- **TSA security guidelines.** TSA's Pipeline Security Branch first issued its voluntary Pipeline Security Guidelines in 2011, and revised them in March 2018. The guidelines include TSA's recommendations for pipeline industry security practices, such as establishing a corporate security program, conducting security vulnerability assessments, and identifying critical facilities. The guidelines also recommend facility security and cybersecurity measures, which serve as the basis for the pipeline security assessments conducted by TSA's Pipeline Security Branch.
- **PHMSA regulations.** PHMSA's Office of Pipeline Safety issues and enforces intrastate and interstate regulations covering aspects of pipeline safety, including the design, construction, operation and maintenance, and spill response for hazardous liquid and gas pipeline facilities, including liquefied natural gas facilities.²⁹
- **Advisory bulletins.** PHMSA also 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. Such bulletins may include identifying the affected operators, describing the threat, and providing information on federal resources for assistance. For example, in response to physical intrusions on pipelines and a coordinated campaign by domestic saboteurs, and to remind pipeline operators of the importance of safeguarding and securing their pipelines from physical and cyber intrusion or attack, PHMSA, in coordination with TSA, issued an advisory bulletin in 2016.³⁰ The bulletin also included a brief discussion of TSA's and PHMSA's roles on pipeline safety and security.
- **Forums and routine interactions with operators.** TSA and PHMSA officials also reported that they communicate their agencies' respective roles and responsibilities for pipeline safety and security to stakeholders when conducting general outreach, information sharing efforts, or inspections or assessments. TSA and PHMSA officials noted that these activities provide opportunities for agency officials and pipeline stakeholders to clarify their roles and responsibilities

²⁹See 49 C.F.R. pts. 190-199.

³⁰In October 2016, environmental activists forced the shutdown of five crude oil pipelines in four states.

should pipeline operators have questions. Examples of such community outreach activities include attending meetings of the Oil and Natural Gas subsector SCC or the Pipeline Modal SCC, and TSA's annual International Pipeline Security Forum.³¹ TSA officials also said that TSA's monthly and quarterly unclassified threat briefings provided TSA officials and pipeline stakeholders the opportunity to discuss and clarify their roles and responsibilities. Additionally, TSA produces classified and unclassified threat assessments on physical and cyber threats to pipelines, which according to agency officials can help to clarify TSA's security role. Finally, TSA and PHMSA officials said that pipeline security assessments and safety inspections and other enforcement activities that the agencies regularly conduct are also opportunities to communicate their roles and responsibilities. For example, TSA officials reported that should an operator ask for assistance regarding a safety issue while TSA staff was conducting a security review, TSA staff would be able to refer the operator to PHMSA to address the issue. Similarly, PHMSA officials stated that inspectors would refer an operator to TSA or its pipeline security guidelines should the operator have questions regarding, for example, what security measures to implement.

The representatives of the four pipeline associations we interviewed reported that TSA and PHMSA had clearly communicated their respective roles and responsibilities to pipeline stakeholders. Specifically, all of the association representatives said that their membership understood that TSA is responsible for pipeline security matters and PHMSA is responsible for pipeline safety matters. For example, one industry association representative stated that they had contacted their members to determine whether they were unclear regarding TSA's and PHMSA's respective roles and responsibilities and that members reported the roles were clear to them. Further, another association representative reported that the initial security reviews and outreach efforts that TSA conducted after the pipeline security program was created helped pipeline operators to understand that its role was to oversee pipeline security.³² In addition, all of the association representatives we interviewed stated that the MOU Annex helped ensure that TSA and PHMSA understood and respected

³¹Pipeline operators may also participate in the Oil and Natural Gas subsector SCC of the Energy SCC.

³²TSA began conducting Corporate Security Reviews in 2003, and Critical Facility Inspections, which are the precursor to its Critical Facility Security Reviews, in 2008.

each other's roles and responsibilities. As a result, according to the association representatives, their pipeline operator membership had not experienced challenges associated with overlapping or duplicative efforts on the part of TSA and PHMSA pipeline safety or security programs.

TSA Communicated Pipeline Incident Response Protocols in Its 2010 Plan, but Has Not Updated the Plan to Address Changes in Key Areas

TSA Has Established a Pipeline Incident Response Protocol Plan That Communicates Agencies' Roles and Responsibilities During Pipeline Incidents

In accordance with the 9/11 Commission Act, TSA issued its *Pipeline Security and Incident Recovery Protocol Plan* in March 2010.³³ The plan's stated intent is to establish a comprehensive interagency approach to counter risks, coordinate federal agencies' actions, and minimize the consequences of incidents involving pipeline infrastructure as well as recovery time from them.³⁴ The plan also defines the roles and responsibilities of federal agencies; tribal, state, and local governments; and the private sector during a pipeline incident. It also defines the measures they may take related to pipeline infrastructure security incidents. According to the plan TSA, PHMSA, the Department of Energy (DOE), and the Federal Bureau of Investigation (FBI) have principal roles in pipeline incident response, while other agencies such as the U.S. Coast Guard, the Federal Emergency Management Agency (FEMA), and the National Transportation Safety Board (NTSB) have supporting roles.

³³See Pub. L. No. 110-53, § 1558, 121 Stat. at 476-47 (requiring the Secretary of Homeland Security, in consultation with the secretary of transportation and the PHMSA Administrator, and in accordance with, among other authorities, the 2006 MOU Annex, to develop a pipeline security and incident recovery protocols plan); 6 U.S.C. § 1208.

³⁴The 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.

The following are examples of agencies' roles and responsibilities in each of the plan's three response phases.

- **Prevention/protection.** TSA is responsible for monitoring pipeline owner and operators' implementation of its pipeline security guidelines, and PHMSA is responsible for enforcing its pipeline safety regulations. TSA, in addition to the FBI, is responsible for assessing the credibility of any physical or cyber threat information it receives and sharing any intelligence related to pipeline security with pipeline owners and operators.
- **Response.** TSA is responsible for coordinating information sharing between federal agencies and pipeline stakeholders, and PHMSA is responsible for coordinating federal agency activities with the affected pipeline operator and state pipeline safety agency. The plan also states that the FBI is responsible for investigating attempted or successful attacks on pipeline infrastructure including those that are believed to have a nexus to terrorism.
- **Recovery.** PHMSA is primarily responsible for working with the pipeline operator, along with other supporting federal agencies, to facilitate service restoration. DOE is responsible for monitoring flows of throughput in the affected pipeline system or systems, assessing regional, national, and global impacts of an incident on energy infrastructure throughout all three phases.

Appendix I provides more details on key federal agencies' and pipeline operators' roles and responsibilities, as well as the actions they may take in response to an incident as detailed in the plan.

TSA Has Not Updated Its Incident Response Plan to Address Changes in Pipeline Security Threats, Technology, and Federal Laws and Policies

TSA's plan states that it will be updated periodically to address changes in pipeline security threats, technology, and federal laws and policies. Further, *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.³⁵ In addition, internal control standards also states that changes in an entity's programs

³⁵[GAO-14-704G](#).

or activities, organizational structure, personnel, or technology can affect the operating environment and management can respond by revising internal controls on a timely basis to ensure effectiveness. However, TSA has not reviewed or revised its 2010 plan to ensure it addresses changes in at least three key areas: cybersecurity-related laws and policies, incident management policies, and DHS's terrorism alert system as described below.

Cybersecurity-related laws and policies

TSA's 2010 plan includes some discussion of cyber threats and refers operators to guidance they may use to better secure their SCADA and control systems.³⁶ However, the plan does not identify the cybersecurity roles and responsibilities of federal agencies that are identified in the plan, such as DOE, Federal Energy Regulatory Commission (FERC), or the FBI, or discuss the measures these agencies should take to prevent, respond to, or support pipeline operators following a cyber incident involving pipelines.³⁷

TSA's 2010 plan also has not been updated to reflect current cybersecurity incident response guidance. In December 2016, DHS issued its National Cyber Incident Response Plan (NCIRP).³⁸ The NCIRP is to be the primary framework for stakeholders, including pipeline operators, to understand how federal departments and agencies provide resources to support response operations for a significant cyber

³⁶The plan refers operators to National Institute of Standards and Technology (NIST) SP 800-82, API's Pipeline SCADA Security Document 1164, and TSA's *Pipeline Security Guidelines*.

³⁷For example, the Fixing America's Surface Transportation Act, enacted in December 2015, designated DOE as the lead sector-specific agency for cybersecurity for the energy sector. See Pub. L. No. 114-94, § 61003(c), 129 Stat. 1312, 1778-79 (2015) (establishing DOE's responsibilities in this capacity to include coordinating with DHS and other relevant federal departments and agencies, collaborating with electric infrastructure owners and operators, among others, prioritizing activities, incident management, responsibilities, and identifying vulnerabilities).

³⁸Department of Homeland Security, National Cybersecurity Incident Response Plan (Washington D.C.: Dec., 2016). DHS issued the NCIRP in accordance with Presidential Policy Directive/PPD-41, which sets forth principles governing the federal government's response to any cyber incident involving government or private sector entities. See White House, *Presidential Policy Directive/PPD-41: United States Cyber Incident Coordination* (Washington D.C.: July 26, 2016).

incident.³⁹ NCIRP identifies the FBI and the National Cyber Investigative Joint Task Force as responsible for investigating reported cyber incidents.⁴⁰ NCIRP also identifies the National Cybersecurity and Communications Integration Center (NCCIC), an agency within DHS, as responsible for providing technical assistance to affected entities, such as pipelines, to mitigate vulnerabilities and reduce impacts of cyber incidents.⁴¹ NCCIC is also to share information across the public and private sectors to protect against similar incidents in the future.

In addition, NCIRP provides guidance detailing when and to which federal agencies or entities the public should report a cyber incident. These include the FBI, the National Cyber Investigative Joint Task Force, U.S. Secret Service, and NCCIC. For example, NCIRP states that any cybercrime—including computer intrusions or attacks, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity—is to be reported to FBI field offices' cyber task forces. However, TSA's plan does not include this information or describe what measures, if any, the agencies with pipeline-related roles and responsibilities listed in NCIRP are to take in response to a pipeline cyber incident.

Moreover, the 2010 plan does not account for other agencies whose roles and responsibilities are related to critical infrastructure, such as pipelines and cybersecurity. Specifically, the plan does not account for the role of NCCIC, which was established in 2009. In addition, TSA's 2010 plan does not account for CISA's role in cyber threat response activities or

³⁹NCIRP defines a significant cyber incident as a cyber incident (or group of related cyber incidents) that is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the nation, or to the public confidence, civil liberties, or public health and safety of the American people.

⁴⁰The Department of Justice, through the FBI and the National Cyber Investigative Joint Task Force, shares investigative information and cyber threat intelligence, as appropriate, with other federal agencies to aid in the analysis of cyber threats and vulnerabilities.

⁴¹NCCIC'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. NCCIC is the federal civilian interface for sharing information related to cybersecurity risks, incidents, analysis, and warnings with federal and nonfederal entities. It provides shared situational awareness to enable real-time actions to address cybersecurity risks and incidents to federal and nonfederal entities.

how it may affect other agencies' roles and responsibilities for pipeline incident response.⁴²

TSA officials acknowledged that reviewing and, as appropriate, revising the plan would be beneficial to ensuring the plan addresses current pipeline security threats, technology, and federal laws and policies. They stated TSA had not updated the plan to include cybersecurity response protocols because an overarching cybersecurity response protocol for all critical infrastructure sectors—not just pipelines—should first be developed. According to TSA officials, developing a pipeline cybersecurity response protocol would require a whole-of-government approach, as well as coordination with private sector and input from many sectors because of the challenges and complexity of critical infrastructure cybersecurity in general.

However, through NCIRP, DHS provided a cybersecurity response protocol across all critical infrastructure sectors in December 2016. Further, NCIRP states that public and private sector entities should consider creating an operational cyber incident response plan to further organize and coordinate their efforts in response to cyber incidents. Therefore, TSA could potentially provide such an operational cyber incident response plan for the pipeline sector in its plan.

TSA could also better ensure that pipeline operators understand how federal agencies may provide support in response to a cyber incident by periodically reviewing and, as appropriate, revising the plan to include its cyber incident response plan. Representatives of the four pipeline associations we interviewed told us that their membership more clearly understood federal agencies' roles and responsibilities related to physical incidents than to cybersecurity. For example, for physical incidents the representatives stated that their members clearly understood that they are to first notify local first responders (often through the emergency 911 system) and appropriate state or federal regulators, and are to contact either the National Response Center or TSA's Transportation Security

⁴²As discussed earlier, the Cybersecurity and Infrastructure Security Agency Act redesignated DHS's National Protection and Programs Directorate as CISA. See Pub. L. No. 115-278, 132 Stat. 4168; 6 U.S.C. § 652. NCCIC, which had been within the National Protection and Programs Directorate, is now a component of CISA.

Operations Center (TSOC),⁴³ depending on the nature of the incident.⁴⁴ However, they stated that they did not believe all of their members clearly understand that they are to report any actual or suspected cyber incidents that could impact pipeline industrial control systems or other information technology-based systems to the NCCIC.⁴⁵ All of the association representatives told us that the process for reporting a cyber incident is less clear because, in part, of the large number of federal agencies with a cybersecurity-related role. One of the representatives also attributed the lack of clarity to the reorganization of NCCIC, and the establishment of CISA. Further, all of the representatives we interviewed indicated that clarifying the cybersecurity roles and responsibilities of DOE, Federal Energy Regulatory Commission (FERC), and TSA would, among other things, improve operators' ability to appropriately report and respond to a cyber incident.

Federal Incident Management Policies

TSA also has not updated the plan to address changes in federal incident management and response policies that have occurred since the plan was developed in 2010. The plan states that it is to be consistent with the National Response Framework (NRF) and the National Incident Management System (NIMS) incident command system procedures.⁴⁶

⁴³The National Response Center is the national point of contact for reporting all oil, chemical, radiological, biological, and etiological discharges into the environment anywhere in the U.S. and its territories. The TSOC is the conduit with which TSA coordinates with DHS, the Federal Aviation Administration, and the FBI 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.

⁴⁴PHMSA requires pipeline operators to report any mechanical failure or unintentional act resulting in significant damage to a pipeline—those that result in serious injury, loss of life, or property damage greater than \$50,000—to PHMSA through the National Response Center. See, e.g., 49 C.F.R. § 195.52. In its *Pipeline Security Guidelines*, TSA requests that pipeline operators report by telephone or email to its 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.

⁴⁵TSA's *Pipeline Security Guidelines* also request that operators report any actual or suspected cyber incidents that could impact pipeline industrial control systems or other information technology-based systems to NCCIC.

⁴⁶The NRF and NIMS are companion documents and are designed to improve the nation's incident management and response capabilities. While the NRF provides the structure and mechanisms for national level policy of incident response, NIMS provides the template for the management of incidents regardless of size, scope or cause.

The NRF was first issued in 2008 and described the roles, responsibilities and coordinating structures for delivering core capabilities during incident response. According to FEMA, it revised the NRF in 2013 and 2016 to reflect lessons learned from real world events and other experiences since the framework was first developed. Likewise, NIMS was developed in 2004 as a comprehensive, national approach to incident management that was to be applicable at all jurisdictional levels and across functional disciplines, such as law enforcement, public health, or public works.⁴⁷ According to FEMA, it revised NIMS in 2017 to reflect and incorporate policy updates and lessons learned from exercises and real-world incidents. The revision was also intended to clarify that NIMS applies to all stakeholders with incident management roles, and to enhance guidance on information management processes, data collection plans, social media integration, and the use of geographic information systems. TSA officials acknowledged the benefit of periodically reviewing, and if necessary, revising the plan to reflect FEMA's revisions to NIMS or the NRF, but had not done so because of competing priorities.

DHS's Terrorism Alert System

TSA has also not updated the plan to address changes DHS made to its terrorist alert system in 2011. Consistent with the 9/11 Commission Act, the plan describes actions that federal agencies can take at each color-coded level of the Homeland Security Advisory System to ensure the increased security of pipeline infrastructure.⁴⁸ For example, under the protect/prevent phase, the plan states that when there is a high risk of a terrorist attack (i.e., red: severe condition) and threat is general and not specific to pipelines, TSA and PHMSA are to coordinate to identify the

⁴⁷NIMS is intended to be applicable across a full spectrum of potential incidents, hazards, and impacts, regardless of size, location or complexity. It is also intended to improve coordination and cooperation between public and private entities in a variety of incident management activities, and provide a common standard for overall incident management. According to FEMA, consistent application of NIMS lays the groundwork for efficient and effective responses, from a single agency fire response to a multiagency, multijurisdictional natural disaster or terrorism response. For more information about NIMS, see FEMA's NIMS website: <https://www.fema.gov/national-incident-management-system>.

⁴⁸Specifically, the 9/11 Commission Act requires that the plan include measures for the federal government to provide increased security support to the most critical interstate and intrastate natural gas and hazardous liquid transmission pipeline infrastructure and operations when under severe security threat levels of alert or when specific security threat information related to such pipeline infrastructure or operations exists. See 6 U.S.C. § 1208(a)(1).

potential for any related or cascading events that may impact the pipeline sector. However, if there is a specific threat to pipelines, TSA, in collaboration with pipeline operators, is to identify any immediate protective measures that pipeline operators are to implement. TSA is also to ensure pipeline operators have the information necessary to implement these measures, and, if necessary, to issue security directives.⁴⁹

In 2011, DHS replaced the four color-coded alert system of the Homeland Security Advisory System with the National Terrorism Advisory System, which has only two alert levels (elevated threat and imminent threat).⁵⁰ TSA issued revised protective measures that pipeline operators are to take under either threat condition in April 2011 and March 2018.⁵¹ However, TSA has not updated the plan to communicate the actions federal agencies can take at either level of the National Terrorism Advisory System to ensure the increased security of pipeline infrastructure.

TSA officials acknowledged that periodically reviewing and, as appropriate, revising the plan would help to clarify federal agencies' roles and responsibilities for addressing pipeline security. TSA officials reported that they have not updated the plan since 2010 because they faced competing priorities. However, as described earlier, TSA's incident response plan was developed to provide a comprehensive interagency approach to important activities such as countering risks, coordinating

⁴⁹If the TSA Administrator determines that a regulation or security directive must be issued immediately in order to protect transportation security, including pipelines, the Administrator is authorized to issue the regulation or security directive without notice or an opportunity to comment. See 49 U.S.C. § 114(l)(2). To date, TSA has not issued a security directive to pipeline operators in response to a terrorist threat.

⁵⁰The National Terrorism Advisory System is DHS's system for communicating terrorist threats to the public. The system is designed to issue bulletins that communicate terrorism information alerting sector stakeholders, including pipeline owners/operators, of any elevated or imminent threats.

⁵¹System alerts take two forms: elevated or imminent. DHS sends elevated threat alerts when there is credible information for which the timing and target of the threat is general, but it is reasonable to recommend implementation of protective measures to thwart or mitigate against an attack. DHS sends imminent threat alerts when there is credible, specific, threat information for which the timing is in the very near term. The protective measures listed are to be implemented when appropriate to the characteristics of their particular facilities, and, to the extent possible, concurrently. See Transportation Security Administration, *Pipeline Security Guidelines: Protective Measures for NTAS Alerts* (Washington, D.C.: March, 2018) (designated by TSA as sensitive security information pursuant to 49 C.F.R. pt. 1520).

federal agencies' actions and minimizing the consequences of incidents involving pipeline infrastructure. Further, the plan itself states that it will be updated periodically to address changes in pipeline security threats, technology, and federal laws and policies.

By periodically reviewing and, as appropriate, revising its *Pipeline Security and Incident Recovery Protocol Plan*, TSA could better ensure that the plan addresses all possible and relevant threats to pipeline systems, such as cybersecurity, and fully incorporates relevant changes, such as those related to incident management and DHS's terrorism alert system. By doing so, TSA could also provide greater assurance that federal agencies understand the actions they are to take to prevent, respond to, or recover from a physical or cyber incident.

Conclusions

TSA and PHMSA share responsibility for safeguarding the nation's pipeline systems from catastrophic events. While the 2006 MOU Annex delineates TSA's and PHMSA's mutually agreed-upon pipeline security roles and responsibilities, it has not been reviewed since its inception to consider pipeline security developments. By developing and implementing a mutually agreed upon timeline with timeframes for reviewing the annex and as appropriate, updating it, TSA and PHMSA could better ensure that their roles and responsibilities are properly documented and updated in a timely manner to remain current. Furthermore, by revising the MOU Annex to include a provision for periodically reviewing the annex for needed updates, TSA and PHMSA could better ensure the agreement consistently reflects relevant and updated information on their roles and responsibilities.

Similarly, TSA's *Pipeline Security and Incident Recovery Protocol Plan*—which defines the roles and responsibilities of federal agencies; tribal, state, and local governments; and the private sector for responding to a pipeline incident—also has not been updated to reflect changes in federal laws or policies since the plan was issued in 2010. By periodically reviewing and, when appropriate, updating its *Pipeline Security and Incident Recovery Protocol Plan*, TSA could better ensure that the plan addresses and fully incorporates changes relevant to cybersecurity, incident management and DHS's terrorism alert system, among others. By doing so, TSA could also 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 preparing for, responding to, or supporting pipeline operators to restore service after a pipeline-related physical or cyber incident.

Recommendations for Executive Action

We are making a total of five recommendations including three to TSA and two to PHMSA:

- The TSA Administrator should work with the PHMSA Administrator to develop and implement a timeline with milestone dates for reviewing and, as appropriate, updating the 2006 MOU Annex. (Recommendation 1)
- The PHMSA Administrator should work with the TSA Administrator to develop and implement a timeline with milestone dates for reviewing and, as appropriate, updating, the 2006 MOU Annex. (Recommendation 2)
- The TSA Administrator, in consultation with the PHMSA Administrator should revise the 2006 MOU Annex to include a provision requiring periodic reviews of, and as appropriate, corresponding updates to the Annex. (Recommendation 3)
- The PHMSA Administrator, in consultation with the TSA Administrator should revise the 2006 MOU Annex to include a provision requiring periodic reviews of, and as appropriate, corresponding updates to the Annex. (Recommendation 4)
- The TSA Administrator should 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. (Recommendation 5)

Agency Comments and Our Evaluation

We provided a draft of this report to DHS and DOT. DHS and DOT provided written comments which are reproduced in appendices III and IV respectively. We also provided draft excerpts of this product to the American Petroleum Institute (API), the American Gas Association, the Interstate Natural Gas Association of America, and the American Public

Gas Association. For those who provided technical comments, we incorporated them as appropriate.

With regard to our first recommendation, that TSA work with the PHMSA to develop and implement a timeline with milestone dates for reviewing and, as appropriate, updating the 2006 MOU Annex, DHS stated that TSA will work with PHMSA to develop and implement a timeline with milestone dates for reviewing and updating, as appropriate, the 2006 MOU Annex. DHS estimated that this effort would be completed by August 31, 2019. This action, if fully implemented, should address the intent of this recommendation.

With regard to our second recommendation, that PHMSA work with TSA to develop and implement a timeline with milestone dates for reviewing and, as appropriate, updating the 2006 MOU Annex, DOT concurred and stated it would provide a detailed response within 180 days of the issuance of this report.

With regard to our third recommendation, that TSA, in consultation with PHMSA, revise the 2006 MOU Annex to include a provision requiring periodic reviews of, and as appropriate, corresponding updates to the Annex, DHS stated that TSA will, in consultation with PHMSA, revise the 2006 MOU Annex to include a provision requiring periodic reviews of, and as appropriate, corresponding updates to the Annex. DHS estimated that this effort would be completed by March 31, 2020. This action, if fully implemented, should address the intent of this recommendation.

With regard to our fourth recommendation, that PHMSA, in consultation with TSA, revise the 2006 MOU Annex to include a provision requiring periodic reviews of, and as appropriate, corresponding updates to the Annex, DOT concurred and stated it would provide a detailed response within 180 days of the issuance of this report.

With regard to our fifth recommendation, that TSA periodically review, and as appropriate, update the 2010 *Pipeline Security and Incident Recovery Protocol Plan* to ensure the plan reflects relevant changes to pipeline security threats, technology, federal law and policy, and any other factors relevant to the security of the nation's pipeline systems, DHS concurred and estimated that TSA will complete its first review by December 31, 2019. DHS further stated that it will establish a timeline for updating the plan should the review determine that an update is necessary. This action, if fully implemented, should address the intent of this recommendation.

We are sending copies of this report to the appropriate congressional committees; the Secretary of Homeland Security, Secretary of Transportation; and other interested parties. In addition, the report will be 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 William Russell 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 report. Key contributors to this report are listed in appendix V.

A handwritten signature in black ink that reads "W. William Russell". The signature is written in a cursive style with a large, prominent initial "W".

W. William Russell
Acting Director, Homeland Security and Justice

Appendix I: 2006 Memorandum of Understanding (MOU) Program Areas and Accompanying Text

The Transportation Security Administration (TSA) and Pipeline and Hazardous Materials Safety Administration (PHMSA), "the parties", recognize that the following program areas are important to the development and deployment of an enhanced security strategy for the transportation of hazardous materials by all modes, including pipeline.

Table 1: 2006 MOU Program Areas and Accompanying Text

Program Area	MOU Annex Text
1. Identification of Critical Infrastructure/Key Resources and Risk Assessments	<p>As a basis for further planning, the parties will review existing definitions of criticality and consider the need, if any, to refine definitions based on known and anticipated risks. To the extent possible, the parties will consider life, safety, economic and environmental impacts, so that the ongoing development of plans and countermeasures for protecting critical infrastructure/key resources (CI/KR) can be prioritized on a risk basis.</p> <p>To support Transportation Security Administration (TSA) efforts in this area, Pipeline and Hazardous Materials Safety Administration (PHMSA) agrees to compliance data, and other information collected in the course of security inspections or reviews of security plans, (including those required under 49 CFR 172.800) and activities of transportation carriers and shippers. PHMSA will provide this data to TSA's Office of Transportation Sector Network Management. Further, PHMSA will coordinate with TSA on observations or recommendations derived from safety inspections and assessments to evaluate whether they conflict with or adversely affect current or planned security requirements.</p> <p>TSA will coordinate with PHMSA on observations or recommended measures derived from the results of criticality and vulnerability assessments, including on pipelines, to evaluate whether they conflict with or adversely affect current or planned safety requirements.</p>
2. Strategic Planning	<p>Security planning will be based on risk. To the extent possible, the parties will seek consensus concerning measures to reduce risk and minimize consequences of emergencies involving critical hazardous materials, transportation packaging, systems and pipeline infrastructure. To promote communications, efficiency and nonduplication of effort, the parties will identify initiatives and activities for achieving performance goals and will develop a program framework and timetable for their completion.</p>

Appendix I: 2006 Memorandum of Understanding (MOU) Program Areas and Accompanying Text

Program Area	MOU Annex Text
3. Standards, Regulations, Guidelines and Directives	<p>In accordance with the MOU, the parties will seek early and frequent coordination in the development standards, regulations, guidelines, or directives affecting transportation security and will work together to obtain any necessary clearance of such documents. In the course of discharging their safety and security missions, the parties will review the adequacy of existing standards in the private and public sector, identifying any gaps that should be addressed through rulemaking, guidelines, or directives. In carrying out this review, the parties will consider private sector investments and resources, identify best practices, and consider opportunities to promote these practices. Where current standards need strengthening, the parties will explore opportunities to build on existing standards-setting activities or processes and are committed to doing so in a manner that minimizes duplication and regulatory burdens.</p> <p>The parties recognize that emergencies or other exigent circumstances may preclude thorough coordination prior to dissemination of these types of measures. The parties will coordinate as extensively as circumstances allow and review actions taken as necessary.</p>
4. Inspections and Enforcement	<p>The parties will explore opportunities for collaboration in inspection and enforcement activities, with the objective of maximizing the use of available resources and targeting enforcement resources on the basis of system risks. The parties will immediately develop procedures for referral of safety and security issues to TSA and PHMSA, respectively; inventory existing inspection and enforcement resources; and develop specific plans for closer coordination in the deployment and use of inspectors, including any necessary additional training.</p>
5. PHMSA Technical Support	<p>The parties recognize that exigent circumstances or other contingencies may tax available security resources. In these situations, TSA may seek to supplement its resources with PHMSA personnel and/or other assets. If TSA determines such support is necessary to develop, staff, implement, or enforce regulations, orders, directives, plans, programs, or other measures, or to conduct security reviews during a period of elevated threat, TSA will request such assistance from PHMSA in writing.</p>
6. Sharing Information During an Emergency Response	<p>The parties participate in established emergency response procedures. However, the parties acknowledge in this Annex that both require timely information during emergencies and commit themselves to promptly sharing information about emergency situations that implicate the missions and interests of the other party. Information in this context includes both the initial incident report and ongoing information about incident developments. The timely sharing of such information serves the public interest in the operation of a secure and safe national transportation system. Each party requires this information to enable the execution of their respective roles in responding to the incident, including dedication of Federal resources, coordinating other forms of assistance and advising the White House or other Federal agencies, as necessary.</p>
7. Public Communication, Education, and Outreach	<p>The parties will build on existing relationships with stakeholders in order to identify and respond to security-related needs and concerns. To these ends, the parties will review existing protocols for public communication concerning security-related matters, specifically including review of existing protocols for publication of information contained in the national pipeline mapping system. The parties also will identify opportunities to improve alignment among themselves and other agencies with related missions.</p>
8. Communicating Protective Measures to Affected Organizations	<p>In pursuit of the joint interest in ensuring the highest state of security and safety awareness and readiness, to the extent practicable, TSA will consult with PHMSA prior to disseminating security requirements (including regulations, orders, and security directives) and voluntary standards and guidelines to the public. Additionally, to the extent practicable, PHMSA will consult with TSA prior to disseminating requirements (including regulations and orders) and voluntary standards and guidelines that impact security to the public.</p>

Appendix I: 2006 Memorandum of Understanding (MOU) Program Areas and Accompanying Text

Program Area	MOU Annex Text
9. Research and Development	The parties will conduct a review of their recently completed and ongoing safety- and security-related projects and identify opportunities to collaborate and support their strategic plan through identification, development, and testing of new or modified technologies or processes. The parties will establish protocols for ongoing information sharing and participation in their respective research and development planning processes.
10. Legislative Matters	In matters affecting pipeline and hazardous material transportation security, the parties will consult with each other as soon as possible on the development of proposed legislation, comments on legislative proposals, draft testimony or briefings to be given before Congressional bodies or staff, and answers to questions for the record.
11. Budget	The parties agree to communicate throughout the budget development, justification, and execution process in order to develop and present a coordinated position on transportation security funding matters and to avoid duplicative requests for funding in connection with pipeline and hazardous material transportation security.

Source: TSA and PHMSA MOU Annex | GAO-19-426

Appendix II: Summary of Key Federal Agencies' and Pipeline Operator's Roles and Responsibilities

This appendix summarizes the roles and responsibilities of key federal agencies as well as the actions that they may take in response to an incident as detailed in Transportation Security Administration's (TSA) 2010 *Pipeline Security and Incident Recovery Protocol Plan*.¹ A summary of pipeline stakeholder's roles, responsibilities, and examples of actions that may be taken during each incident response phase is presented below.

- **Prevention/Protection.** During the prevention/protection phase, pipeline operators are to use TSA's pipeline security guidance and the Pipeline and Hazardous Materials Safety Administration's (PHMSA) safety regulations as the framework to prepare and prevent against an incident. TSA is responsible for monitoring pipeline owners and operators' implementation its security guidelines, and PHMSA is responsible for enforcing its safety regulations. The plan also states that during this phase TSA is to assume a primary role for ensuring federal agencies' actions are coordinated through protective security advisors (PSAs).² In addition, the Federal Bureau of Investigation (FBI) is responsible for assessing the credibility of a known threat, preparing and implementing a preliminary investigative plan, and, if necessary, disseminating public safety notifications. The Department

¹The plan is organized into three main components corresponding to the incident phases: prevention/protection, response, and recovery.

²PSAs 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.

of Energy (DOE) is responsible for assessing and monitoring pipeline systems for supply shortages.

The prevention/protection section of the plan also describes how agencies are to share and assess threat information. For example, the plan states that TSA, PHMSA, or any federal agency that receives threat information regardless of the source, must immediately notify the FBI.³ It also states that if the FBI receives intelligence about a pipeline threat, it is to share this information with TSA. TSA is then to notify the pipeline operator and, if necessary, provide recommendations for additional protective measures.

Finally, the prevention/protection section of the plan defines actions various agencies can implement during a heightened security threat level to increase protection from a potential attack.⁴ For example, when there is a high risk of a terrorist attack (i.e., red: severe condition) and threat is general and not specific to pipelines, TSA and PHMSA are to coordinate to identify the potential for any related or cascading events that may impact the pipeline sector. If there is a specific threat to pipelines, TSA is, in collaboration with pipeline operators, to identify any immediate protective measures that ought to be taken by pipeline operators, and ensure pipeline operators have the information necessary to implement them, and, if necessary issue security directives.⁵

³According to TSA Intelligence and Analysis officials, TSA operates under the assumption that this does not apply to any generally available threat messaging to which TSA and the FBI both have access. Currently, according to them, TSA has limited access to any operational information or intelligence held by the FBI.

⁴The Implementing Recommendations of the 9/11 Commission Act of 2007 requires that the plan include measures for the federal government to provide increased security support to the most critical interstate and intrastate natural gas and hazardous liquid transmission pipeline infrastructure and operations when under severe security threat levels of alert or when specific security threat information related to such pipeline infrastructure or operations exists. See Pub. L. No. 110-53, § 1558, 121 Stat. 266, 476-47 (2007); 6 U.S.C. § 1208. The plan describes actions that can be taken at each Homeland Security Advisory System (HSAS) color-coded level to ensure the increased security of pipeline infrastructure. In 2011, the Department of Homeland Security (DHS) replaced the color-coded alerts of the Homeland Security Advisory System (HSAS) with the National Terrorism Advisory System (NTAS).

⁵If the TSA Administrator determines that a regulation or security directive must be issued immediately in order to protect transportation security, including pipelines, the Administrator is authorized to issue the regulation or security directive without notice or an opportunity to comment. See 49 U.S.C. § 114(l)(2). To date, TSA has not issued a security directive to pipeline operators in response to a terrorist threat.

- **Response.** According to the plan, pipeline owners or operators are to notify local first responders and state regulators through the emergency 911 system. After the pipeline operator has notified local government, they are to contact the National Response Center (NRC) if the incident results in an unintentional release or causes significant damage.⁶ As we previously reported, pipeline operators are also requested to report any physical security incident that is indicative of a deliberate attempt to disrupt pipeline operations or activities that could be considered precursors to such an attempt to TSA's Transportation Security Operations Center (TSOC).⁷ Once TSA has been notified of an incident by a pipeline operator, its Pipeline Security Branch is to monitor the incident, notify relevant federal agencies, and, if deemed appropriate, activate the Interagency Threat Coordination Committee (ITCC).⁸ PHMSA may also deploy on-scene pipeline inspectors and investigators which are to among other things, coordinate federal agencies' activities with the affected pipeline operator and state pipeline safety agency, provide subject matter expertise to the incident command, and direct safe restoration of pipeline facilities and services.

The plan also states that, during the response phase, responsibility for investigating the incident falls to NTSB or the FBI depending on

⁶PHMSA requires transmission pipelines carrying liquid or gas that could affect a high consequence area to have written plans that address pipeline risks, baseline assessments of line pipe, identification of pipeline segments that may affect a high consequence area, as well as a method to ensure continual evaluation of the pipeline to maintain its integrity. See 49 C.F.R. § 195.452 (for liquids) and 49 C.F.R. pt. 192, subpt. O (for gas). Further, any mechanical failure or unintentional act that results in significant damage to a pipeline—those resulting in serious injury, loss of life, or property damage greater than \$50,000—are to be reported to PHMSA through DOT's National Response Center (NRC). See, e.g., 49 C.F.R. § 195.52.

⁷See [GAO-19-48](#). 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 NCCIC.

⁸The ITCC is designed to organize and communicate developing threat information among federal agencies at the headquarters-level that may have responsibilities during a pipeline incident response to avoid duplication or overlap in agencies' responses. It also is to identify any type of assistance that may be useful to pipeline operators and provide threat information. It is composed of TSA's Pipeline Security Branch, TSA Intelligence & Analysis, PHMSA, DOT's Office of Intelligence, Security, and Emergency Response; DOE; and the FBI. However, it may also include other government entities, including state governments, with specific expertise and authorities, as necessary.

whether the incident is determined to be the result of criminal activity.⁹ The FBI is solely responsible for investigating any pipeline security incident that appears to be an intentional criminal act.¹⁰ For example, if the incident were suspected to be the result of terrorist attack, the National Joint-Terrorism Task Force would conduct an investigation of the attack, and if appropriate, with assistance from other FBI assets.¹¹ If, however, the incident resulted in fatalities, substantial property damage, or significant injury to the environment, NTSB would have responsibility for investigating the incident, and may issue safety recommendations to help prevent future accidents.¹²

- **Recovery.** When response activities are complete, PHMSA is to have primary responsibility for overseeing pipeline operators' safe restoration of service with TSA and other federal agencies serving primarily in support roles. PHMSA, for example, is to work with the owner/operator to facilitate restoration of service by, among other things, providing technical oversight, advice, and guidance to owner/operators; coordinating recovery activities with state pipeline safety agency, and evaluate whether to a special permit is necessary to facilitate an expedited restoration of services. Meanwhile, DOE is to continue to assess the impacts of an incident on energy infrastructure, and advise federal, state, tribal, and local authorities on priorities for energy restoration, assistance, and supply.

⁹According to PHMSA officials, DOT's Office of Inspector General is to investigate criminal violations of the Pipeline Safety Act, which includes intentionally damaging or destroying pipeline facilities. See e.g., 49 U.S.C. § 60123(b).

¹⁰The plan states that TSA, PHMSA, or any federal agency that receives threat information regardless of the source, must immediately notify the FBI.

¹¹The National Joint Terrorism Task Force is responsible for managing FBI's Joint Terrorism Task Force program and coordinating the efforts of regional task forces. Joint Terrorism Task Forces work to prevent, preempt, deter, and investigate terrorism and related activities affecting the United States as well as to apprehend terrorists. They consist of law enforcement and other specialists from federal, state, and local law enforcement and intelligence agencies, and are led by the Department of Justice and the FBI.

¹²The NTSB is an independent federal agency responsible for investigating transportation accidents. See generally 49 U.S.C. §§ 1111, 1131. For example, the NTSB has discretion to investigate pipeline accidents but must investigate those involving a fatality, substantial property damage, or significant injury to the environment.

Appendix III: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528



Homeland
Security

May 22, 2019

Mr. William Russell
Acting Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

RE: Management Response to Draft Report: GAO-19-426, "CRITICAL
INFRASTRUCTURE PROTECTION: Key Pipeline Security Documents Need to
Reflect Current Operating Environment"

Dear Mr. Russell:

Thank you for the opportunity to comment on this 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 appreciates GAO's recognition of the continuing close partnership between the Transportation Security Administration (TSA) and the Department of Transportation's (DOT) Pipeline and Hazardous Materials Safety Administration (PHMSA), and notes there was no confusion according to pipeline industry representatives about agency roles and responsibilities for safety and security. The draft report also acknowledged that TSA and PHMSA work together closely to implement their respective authorities to ensure the safety and security of the hazardous liquid and natural gas pipeline infrastructure in the United States. This includes collaboration in response to significant pipeline incidents as well as natural hazards, such as hurricanes. DHS remains committed to working with its Federal and private sector partners in ensuring the security and resilience of our Nation's critical pipeline infrastructure.

To further facilitate this cooperative working relationship, TSA and PHMSA began an effort in 2018 to update the Annex to the 2006 Memorandum of Understanding (MOU) between DHS and DOT, which delineates lines of authority and responsibility between the agencies on pipeline and hazardous materials transportation security. This project was temporarily put on hold pending completion of this GAO review so that the update could reflect the results of the GAO's analysis and recommendations. TSA will re-engage with PHMSA to update the Annex to the MOU to reflect the current operating

environment. Although significantly more challenging, TSA will also begin a review and update to the 2010 Pipeline Security and Incident Recovery Protocol Plan, as appropriate.

The draft report contained five recommendations, including three for TSA (Recommendations 1, 3, and 5) and two for PHMSA (Recommendations 2 and 4). DHS concurs with the recommendations to TSA. Attached find our detailed response to each of these recommendations. 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 with any questions, and 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-19-426**

GAO recommended that the TSA Administrator:

Recommendation 1: Work with the PHMSA Administrator to develop and implement a timeline with milestone dates for reviewing and, as appropriate, updating the 2006 MOU Annex.

Response: Concur. TSA's Office of Policy, Plans and Engagement will work with PHMSA to develop and implement a timeline with milestone dates for reviewing and updating, as appropriate, the 2006 MOU Annex. Estimated Completion Date (ECD): August 31, 2019.

Recommendation 3: 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.

Response: Concur. In consultation with PHMSA, TSA's Office of Policy, Plans and Engagement will revise the 2006 MOU Annex to include a provision requiring periodic reviews of, and as appropriate, corresponding updates to the Annex. ECD: March 31, 2020.

Recommendation 5: Periodically review, and as appropriate, update the 2010 Pipeline Security and Incident Recovery Protocol Plan to ensure the plan reflects relevant changes to pipeline security threats, technology, federal law and policy, and any other factors relevant to the security of the nation's pipeline systems.

Response: Concur. TSA's Office of Policy, Plans and Engagement will 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. The first review will be completed by December 31, 2019. A timeline for completing an update will then be established if the review results in a decision that an update is necessary. ECD: To Be Determined.

Text of Appendix III: Comments from the Department of Homeland Security

Page 1

May 22, 2019

Mr. William Russell

Acting Director, Homeland Security and Justice

U.S. Government Accountability Office 441 G Street, NW

Washington, DC 20548

RE: Management Response to Draft Report: GAO-19-426 , "CRITICAL
INFRASTRUCTURE PROTECTION: Key Pipeline Security Documents Need to
Reflect Current Operating Environment"

Dear Mr. Russell:

Thank you for the opportunity to comment on this 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 appreciates GAO's recognition of the continuing close partnership between the Transportation Security Administration (TSA) and the Department of Transportation's (DOT) Pipeline and Hazardous Materials Safety Administration (PHMSA), and notes there was no confusion according to pipeline industry representatives about agency roles and responsibilities for safety and security. The draft report also acknowledged that TSA and PHMSA work together closely to implement their respective authorities to ensure the safety and security of the hazardous liquid and natural gas pipeline infrastructure in the United States. This includes collaboration in response to significant pipeline incidents as well as natural hazards, such as hurricanes. DHS remains committed to working with its Federal and private sector partners in ensuring the security and resilience of our Nation's critical pipeline infrastructure.

To further facilitate this cooperative working relationship, TSA and PHMSA began an effort in 2018 to update the Annex to the 2006 Memorandum of Understanding (MOU) between DHS and DOT, which delineates lines of authority and responsibility

between the agencies on pipeline and hazardous materials transportation security. This project was temporarily put on hold pending completion of this GAO review so that the update could reflect the results of the GAO's analysis and recommendations. TSA will re-engage with PHMSA to update the Annex to the MOU to reflect the current operating

Page 2

environment. Although significantly more challenging, TSA will also begin a review and update to the 2010 Pipeline Security and Incident Recovery Protocol Plan, as appropriate.

The draft report contained five recommendations, including three for TSA (Recommendations 1, 3, and 5) and two for PHMSA (Recommendations 2 and 4). DHS concurs with the recommendations to TSA. Attached find our detailed response to each of these recommendations. 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 with any questions, and we look forward to working with you again in the future.

Sincerely,

Jim H. Crumpacker

Director

Departmental GAO-OIG Liaison Office

Attachment

Page 3

Attachment: Management Response to Recommendations Contained in GAO-19-426

GAO recommended that the TSA Administrator:

Recommendation 1: Work with the PHMSA Administrator to develop and implement a timeline with milestone dates for reviewing and, as appropriate, updating the 2006 MOU Annex.

Response: Concur.

TSA's Office of Policy, Plans and Engagement will work with PHMSA to develop and implement a timeline with milestone dates for reviewing and updating, as appropriate, the 2006 MOU Annex. Estimated Completion Date (ECD): August 31, 2019.

Recommendation 3: 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.

Response: Concur.

In consultation with PHMSA, TSA's Office of Policy, Plans and Engagement will revise the 2006 MOU Annex to include a provision requiring periodic reviews of, and as appropriate, corresponding updates to the Annex. ECD: March 31, 2020.

Recommendation 5: Periodically review, and as appropriate, update the 2010 Pipeline Security and Incident Recovery Protocol Plan to ensure the plan reflects relevant changes to pipeline security threats, technology, federal law and policy, and any other factors relevant to the security of the nation's pipeline systems.

Response: Concur.

TSA's Office of Policy, Plans and Engagement will 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. The first review will be completed by December 31, 2019 . A timeline for completing an update will then be established if the review results in a decision that an update is necessary. ECD: To Be Determined.

Appendix IV: Comments from the Department of Transportation



**U.S. Department
of Transportation**

Office of the Secretary
of Transportation

1200 New Jersey Avenue, SE
Washington, DC 20590

Bill Russell
Director, Homeland Security and Justice Issues
U.S. Government Accountability Office (GAO)
441 G Street NW
Washington, D.C. 20548

MAY 16 2019

Dear Mr. Russell:

The Pipeline and Hazardous Materials Safety Administration's (PHMSA) mission is to protect people and the environment by advancing the safe transportation of energy and other hazardous materials that are essential to our daily lives. PHMSA is responsible for developing and enforcing regulations to support safe, reliable, and environmentally sound pipeline transportation in the United States. As a part of its safety mission, PHMSA shares responsibility for safeguarding the nation's pipeline system with the Department of Homeland Security's (DHS) Transportation Security Administration (TSA), and pipeline owners and operators.

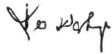
Pursuant to a September 2004 Memorandum of Understanding (MOU) between the Department of Transportation (DOT) and DHS, PHMSA and TSA signed an Annex in August 2006 to further delineate the roles and responsibilities between the agencies on pipeline and hazardous materials transportation security. PHMSA recognizes the value of the 2006 Annex and acknowledges the need to revise the document. PHMSA's Administrator directed PHMSA staff to review the Annex and collaborate with its TSA partners to update the document. Since early 2018, PHMSA and TSA have met to review the Annex and identified outdated references to certain Presidential Policy Directives and legal citations, as well as sections requiring revision to more accurately reflect current programs.

Upon review of the draft report, PHMSA concurs with GAO's two recommendations to: (1) work with TSA to develop and implement a timeline with milestone dates for reviewing and updating the 2006 Annex; and (2) include a provision requiring periodic reviews of and appropriate updates to the Annex to ensure that it stays current with legal and policy developments. DOT will provide a detailed response to the recommendations within 180-days of the final report's issuance.

**Appendix IV: Comments from the Department
of Transportation**

PHMSA appreciates the opportunity to respond to the GAO draft report. Please contact Madeline M. Chulumovich, Director of Audit Relations and Program Improvement, at (202) 366-6512 with any questions or if GAO would like additional information.

Sincerely,



Keith Washington
Deputy Assistant Secretary for Administration

**Appendix IV: Comments from the Department
of Transportation**

Text of Appendix IV: Comments from the Department of Transportation

Page 1

MAY 16, 2019

Bill Russell

Director, Homeland Security and Justice Issues

U.S. Government Accountability Office (GAO) 441 G Street NW

Washington, D.C. 20548

Dear Mr. Russell:

The Pipeline and Hazardous Materials Safety Administration's (PHMSA) mission is to protect people and the environment by advancing the safe transportation of energy and other hazardous materials that are essential to our daily lives. PHMSA is responsible for developing and enforcing regulations to support safe, reliable, and environmentally sound pipeline transportation in the United States. As a part of its safety mission, PHMSA shares responsibility for safeguarding the nation's pipeline system with the Department of Homeland Security's (DHS) Transportation Security Administration (TSA), and pipeline owners and operators.

Pursuant to a September 2004 Memorandum of Understanding (MOU) between the Department of Transportation (DOT) and DHS, PHMSA and TSA signed an Annex in August 2006 to further delineate the roles and responsibilities between the agencies on pipeline and hazardous materials transportation security. PHMSA recognizes the value of the 2006 Annex and acknowledges the need to revise the document. PHMSA's Administrator directed PHMSA staff to review the Annex and collaborate with its TSA partners to update the document. Since early 2018, PHMSA and TSA have met to review the Annex and identified outdated references to certain Presidential Policy Directives and legal citations, as well as sections requiring revision to more accurately reflect current programs.

Upon review of the draft report, PHMSA concurs with GAO's two recommendations to: (1) work with TSA to develop and implement a timeline with milestone dates for reviewing and updating the 2006 Annex; and (2) include a provision requiring periodic reviews of and appropriate updates to the Annex to ensure that it stays

current with legal and policy developments. DOT will provide a detailed response to the recommendations within 180-days of the final report's issuance.

Page 2

PHMSA appreciates the opportunity to respond to the GAO draft report. Please contact Madeline M. Chulumovich, Director of Audit Relations and Program Improvement, at (202) 366-6512 with any questions or if GAO would like additional information.

Sincerely,

Keith Washington

Deputy Assistant Secretary for Administration

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

Bill Russell at (202) 512-8777 or russellw@gao.gov

Staff Acknowledgments

In addition to the contact named above, Ben Atwater, Assistant Director and Michael C. Lenington, Analyst-in-Charge, managed this assignment. Nanette Barton, Eric Hauswirth, Susan Hsu, and Thomas Lombardi also 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 FraudNet:

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.