United States Government Accountability Office

GAO

Report to Congressional Committees

August 2010

PIPELINE SECURITY

TSA Has Taken Actions to Help Strengthen Security, but Could Improve Priority-Setting and Assessment Processes

GAO
Accountability * Integrity * Reliability

GAO
Accountability·Integrity·Reliability
Highlights

Highlights of GAO-10-867, a report to congressional committees

Why GAO Did This Study

The United States depends on a vast network of pipelines to transport energy. GAO was asked to review the Transportation Security Administration's (TSA) efforts to help ensure pipeline security. This report addresses the extent to which TSA's Pipeline Security Division (PSD) has (1) assessed risk and prioritized efforts to help strengthen pipeline security, (2) implemented agency guidance and requirements of the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act) regarding pipeline security, and (3) measured its performance in strengthening pipeline security. GAO reviewed PSD's risk assessment process and performance measures and observed 14 PSD reviews and inspections scheduled during the period of GAO's review. Although these observations are not generalizable, they provided GAO an understanding of how PSD conducts reviews and inspections.

What GAO Recommends

GAO recommends that TSA, among other things, establish time frames for improving risk model data, document its method for scheduling reviews, develop a plan for transmitting recommendations to operators, follow up on its recommendations, include performance measures linked to objectives in its pipeline strategy, and develop more outcome measures. DHS concurred with the recommendations and discussed planned actions, but not all will fully address the recommendations, as discussed in the report.

View GAO-10-867 or key components.
For more information, contact Steve Lord at (202) 512-4379 or lords@gao.gov.

August 2010

PIPELINE SECURITY

TSA Has Taken Actions to Help Strengthen Security, but Could Improve Priority-Setting and Assessment Processes

What GAO Found

PSD identified the 100 most critical pipeline systems and developed a pipeline risk assessment model based on threat, vulnerability, and consequence, but could improve the model's consequence component and better prioritize its efforts. The consequence component takes into account the economic impact of a possible pipeline attack, but not other possible impacts such as public health and safety, as called for in the Department of Homeland Security's (DHS) risk management guidance. PSD plans to improve its model by adding more vulnerability and consequence data, but has no time frames for doing so. Establishing a plan with time frames, as called for by standard management practices, could help PSD enhance the data in, and use of, its risk assessment model. Also, PSD procedures call for scheduling Corporate Security Reviews (CSR)—assessments of pipeline operators' security planning—based primarily on a pipeline system's risk, but GAO's analysis of CSR data suggests a system's risk was not the primary consideration. Documenting a methodology for scheduling CSRs that includes how to balance risk with other factors could help PSD ensure it prioritizes its oversight of systems at the highest risk.

PSD has taken actions to implement agency guidance that outlines voluntary actions for pipeline operators and 9/11 Commission Act requirements for pipeline security, but lacks a system for following up on its security recommendations to pipeline operators. PSD established CSR and Critical Facility Inspection (CFI) Programs in 2003 and 2008, respectively, and has completed CSRs of the 100 most at-risk systems, started conducting second CSRs, and completed 224 of 373 one-time CFIs. Both programs result in recommendations, but PSD does not generally send CSR recommendations to operators in writing or follow up to ensure that CSR and CFI recommendations were implemented. Standard project management practices call for plans that define approaches and start dates and Standards for Internal Control in the Federal Government calls for monitoring to ensure review findings are resolved. Developing a plan for how and when PSD will begin transmitting CSR recommendations to operators, and following up on CSR and CFI recommendations could better inform PSD of the state of pipeline security and whether operators have addressed vulnerabilities.

PSD has taken steps to gauge its progress in strengthening pipeline security, but its ability to measure improvements is limited. In its pipeline security strategy, PSD does not include performance measures or link them to objectives, which GAO previously identified as desirable in security strategies. In addition, PSD developed performance measures, including one outcome measure to gauge its efforts to help operators reduce vulnerabilities identified in CSRs. However, the outcome measure does not link to all three of PSD's objectives and provides limited information on improvements in areas such as physical security. According to DHS risk management guidance, outcome measures should link to objectives. Including measures linked to objectives in its strategy and developing more outcome measures directly linked to all of its objectives could help PSD improve accountability and assess improvements.

Contents

Table

Figures

Abbreviations

AGA	American Gas Association
AOPL	Association of Oil Pipe Lines
APGA	American Public Gas Association
API	American Petroleum Institute
CFI	Critical Facility Inspection
CSR	Corporate Security Review
DOE	Department of Energy
DHS	Department of Homeland Security
DOT	Department of Transportation
FBI	Federal Bureau of Investigation
FMFIA	Federal Managers' Financial Integrity Act of 1982
HSPD-7	Homeland Security Presidential Directive-7
INGAA	Interstate Natural Gas Association of America
MOU	memorandum of understanding
NIPP	National Infrastructure Protection Plan
PHMSA	Pipeline and Hazardous Materials Safety Administration
PSD	Pipeline Security Division
TSA	Transportation Security Administration
TSNM	Office of Transportation Sector Network Management

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.

GAO

Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

August 4, 2010

The Honorable John Rockefeller
Chairman
The Honorable Kay Bailey Hutchison
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Frank R. Lautenberg
Chairman
The Honorable John Thune
Ranking Member
Subcommittee on Surface Transportation and Merchant Marine
Infrastructure, Safety, and Security
Committee on Commerce, Science, and Transportation
United States Senate

U.S. citizens and businesses depend on the continued operation of vast networks of pipelines that traverse hundreds of thousands of miles to transport energy for operating air and surface vehicles, running industrial equipment, heating homes, and generating electricity. The United States has the largest network of energy pipelines of any nation in the world. These pipelines transport nearly all the natural gas and about two-thirds of the hazardous liquids, including crude and refined petroleum products, consumed in the United States, making them a potential target to those wanting to disrupt commerce and other activities. Although attacks on U.S. pipelines have been rare—carried out, for example, by individuals with unclear motives—attacks on pipelines outside the United States by groups such as militant rebels highlight potential vulnerabilities of pipelines. For example, in Colombia, rebels attacked a major pipeline using explosives more than 600 times from 1996 through 2005, and in Nigeria, militant rebels have repeatedly attacked pipelines and oil facilities. Within the United States, a terrorist plot to attack jet fuel pipelines and storage tanks at JFK International Airport was uncovered and foiled in 2007. The same year, a U.S. citizen was convicted of attempting to provide material support to terrorists, among other things, after he tried to conspire with Al-Qaeda to blow up sections of the Trans Alaska Pipeline System and sections of the Transcontinental Pipeline System, which carries natural gas from the Gulf Coast to New York City. Such events raise concerns that attacks could occur in the United States.

Securing the nation's pipeline system is a responsibility shared by the federal government and the private sector. Prior to the terrorist attacks of September 11, 2001, the federal government's involvement in pipelines largely focused on safety, and security efforts were minimal. In November 2001, the Aviation and Transportation Security Act established the Transportation Security Administration (TSA) within the Department of Transportation (DOT) and gave TSA the lead responsibility for security in all modes of transportation, including pipeline.[1] In November 2002, the Homeland Security Act was enacted, and upon the creation of the Department of Homeland Security, TSA was transferred from DOT to DHS, where it currently resides.[2] In August 2007, the federal government enacted the Implementing Recommendations of the 9/11 Commission Act of 2007, which required the Secretary of Homeland Security, in consultation with the Secretary of Transportation, to take specific pipeline security actions.[3] Within DHS, TSA's Pipeline Security Division (PSD) leads pipeline security activities. TSA has not issued pipeline security regulations, but works with the pipeline industry to implement suggested security measures to make pipeline systems more secure. Private companies who own and operate pipeline systems are responsible for assessing their own specific security needs and incur the costs associated with implementing security measures.

Since it is not feasible to protect all assets and systems against every possible threat, DHS has called for using a risk management approach to prioritize its investments, develop plans, and allocate resources in a risk-informed way that balances security and commerce. DHS detailed this approach in its National Infrastructure Protection Plan (NIPP), which it issued in June 2006 and updated in 2009.[4]

[1] Pub. L. No. 107-71, 115 Stat. 597 (2001).

[2] Pub. L. No. 107-296, 116 Stat. 2135 (2002).

[3] Pub. L. No. 110-53, 121 Stat. 266 (2007). The 9/11 Commission was a congressionally chartered commission established by Congress on November 27, 2002, to (1) investigate the relevant facts and circumstances relating to the terrorist attacks of September 11, 2001; (2) identify, review, and evaluate lessons learned from these attacks; and (3) report to the President and the Congress on findings, conclusions, and recommendations that generated from the investigation and review.

[4] The NIPP provides a unifying structure for the integration of a range of efforts for the protection and resilience of the nation's critical infrastructure and key resources.

You requested that we review TSA's efforts to help ensure pipeline security. Specifically, this report addresses the following objectives:

- To what extent has TSA's Pipeline Security Division (PSD) identified critical pipeline systems, assessed risk, and prioritized efforts, consistent with the NIPP, to help strengthen the security of hazardous liquid and natural gas pipeline systems?
- To what extent has PSD taken actions to implement agency guidance and requirements of the Implementing Recommendations of the 9/11 Commission Act of 2007 regarding the security of hazardous liquid and natural gas pipeline systems?
- To what extent has PSD measured its performance to help strengthen the security of hazardous liquid and natural gas pipeline systems and improvements in pipeline security?

To determine the extent to which PSD used a risk management process to help strengthen the security of pipelines, we reviewed PSD's efforts to identify critical pipeline systems, assess risk, and prioritize its pipeline review efforts.[5] We reviewed relevant documents, including PSD's list of the 100 most critical pipeline systems, and interviewed PSD officials about the methods they used to identify these systems.[6] We reviewed TSA assessments of threat, vulnerability, and consequence from 2003 through May 2010—such as TSA's annual pipeline threat assessment, Corporate Security Reviews (CSR) that PSD uses as a vulnerability assessment, and consequence assessments on natural gas disruptions sponsored by the Department of Energy (DOE) and PSD—and discussed these with relevant agency officials.[7] TSA characterized these as threat, vulnerability, and consequence assessments, but we did not assess the extent to which these

[5] Throughout this report, we use the term pipelines to refer to either hazardous liquid or natural gas pipelines.

[6] A system is considered critical if it is so vital to the United States that its incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof. PSD determined the most critical pipeline systems based on the amount of energy they carry.

[7] Corporate Security Reviews are on-site reviews to assess corporate security plans for pipeline systems. The intent of these reviews is to develop first-hand knowledge of security planning, establish working relationships with key pipeline security personnel, and identify and share good security practices. PSD has conducted CSRs for the 100 most critical pipeline systems.

assessment activities met the NIPP criteria for such assessments, as this was outside the scope of our work. We analyzed PSD's risk assessment model, which integrates the various assessments to develop a risk estimate and relative risk ranking for each pipeline system, and the data PSD inputs into the model. We also compared the time elapsed between PSD's first and subsequent CSRs for each pipeline system with the system's ranking based on risk to measure the strength of their relationship. Additionally, we compared the order in which PSD conducted the first Critical Facility Inspection (CFI) for each system with each system's risk ranking, and measured the strength of that relationship.[8] To assess the reliability of April 2003 through May 2010 risk assessment model data, we (1) performed testing of required data elements, (2) compared the data with other sources of information, and (3) interviewed knowledgeable agency officials. We determined that the data were sufficiently reliable for the purposes of this report. We analyzed agency guidance on risk management, including the NIPP and the Transportation Systems Sector-Specific Plan, to determine criteria for effectively implementing a risk management framework and associated best practices for conducting risk assessments, and compared these with PSD's risk management strategy.[9] We also compared PSD's approach for advancing its risk management program to standard practices in program management planning.[10]

To determine the extent to which PSD has taken actions to implement agency guidance and Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act) requirements regarding pipeline security, we reviewed the Pipeline Security Information Circular

[8] PSD established a program for inspecting all the critical facilities of the 100 most critical pipeline systems, as required by the Implementing Recommendations of the 9/11 Commission Act. These physical inspections include the interior and exterior of each critical facility.

[9] The NIPP obligates each sector to develop a sector-specific plan that describes strategies to protect the nation's critical infrastructure and key resources under its purview, outline a coordinated approach to strengthen security efforts, and determine appropriate programmatic funding levels. TSA, as the sector-specific agency for the transportation sector, developed the Transportation Systems Sector-Specific Plan, which describes the strategies to protect all modes of transportation (aviation, maritime, mass transit, highway, freight rail, and pipeline).

[10] The Project Management Institute, *The Standard for Program Management* © (2006).

(2002 circular)[11] and the 9/11 Commission Act and actions described in agency documents.[12] To learn more about PSD's actions, we interviewed officials from PSD and DOT as well as representatives of the major associations with ties to the pipeline industry (American Petroleum Institute, Association of Oil Pipe Lines, American Gas Association, Interstate Natural Gas Association of America, and American Public Gas Association); attended the 2008 International Pipeline Security Forum organized by PSD and Natural Resources Canada; and met with security personnel from 10 pipeline operators with headquarters or significant operations in Houston.[13] We chose Houston because it has the highest concentration of operators with systems on PSD's list of the 100 most critical pipeline systems, and those with whom we met operate about one-third of those systems. While the results of these interviews cannot be generalized to all pipeline operators and industry associations, they provided perspectives on how operators view PSD's security efforts. Further, we accompanied PSD officials on 4 reviews of pipeline systems operated by 4 different operators and 10 inspections of critical facilities operated by 3 different operators. We observed these reviews and inspections because PSD had scheduled them while we were conducting our work. These involved hazardous liquid and natural gas pipelines as well as different size operators with pipeline systems that varied in the amount of energy they carry, their relative risk ranking, and their location (we observed CSRs in four states and CFIs in three states). While the results of these observations cannot be generalized to all CSRs and CFIs or all pipeline systems and critical facilities, they provided us with an understanding of how PSD conducts these reviews and inspections, and some perspective on the security posture at different critical facilities. We also interviewed representatives of Secure Solutions International—a security and risk management consulting firm that assisted PSD in developing and carrying out CFIs—about critical facilities and the inspection process. In addition, we independently observed the exterior of

[11] The 2002 circular outlines voluntary actions that pipeline operators should take and describes actions the federal government plans to take to improve pipeline security. We also reviewed the Pipeline Security Contingency Planning Guidance, which is considered part of the 2002 circular.

[12] Documents we reviewed included PSD's Pipeline Modal Annex, CSR Standard Operating Procedures, CSR and Critical Facility Inspection (CFI) protocols, and Pipeline Security Smart Practices.

[13] Natural Resources Canada is the Canadian government agency that seeks to enhance the responsible development and use of Canada's natural resources and the competitiveness of Canada's natural resources products.

10 other critical facilities. We selected these facilities, which were located in four states and operated by 6 different operators, because of their proximity to our offices. Although the results of these observations cannot be generalized to all critical facilities, they provided us insight on security measures at additional critical facilities. We compared PSD's processes for transmitting and following up on CSR and CFI recommendations with criteria in GAO Standards for Internal Control in the Federal Government regarding recording and communicating deficiencies found during evaluations.[14] We also compared PSD's approach for advancing its process for communicating CSR recommendations to standard practices in project management.[15]

To determine the extent to which PSD measured its performance in strengthening the security of pipelines and improvements in pipeline security, we reviewed PSD's performance measures and interviewed Office of Transportation Sector Network Management and PSD officials regarding those measures, and discussed PSD's related data collection methodologies with PSD officials.[16] We analyzed TSA's national security strategy for pipeline systems—the Pipeline Modal Annex—to determine the extent to which it conformed to provisions related to goal setting and performance measurement found in Executive Order 13416: Strengthening Surface Transportation Security,[17] the NIPP, the Transportation Systems

[14] GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999). These standards, issued pursuant to the requirements of the Federal Managers' Financial Integrity Act of 1982 (FMFIA), provide the overall framework for establishing and maintaining internal control in the federal government. Also pursuant to FMFIA, the Office of Management and Budget issued Circular A-123, revised December 21, 2004, to provide the specific requirements for assessing the reporting on internal controls. Internal control standards and the definition of internal control in Circular A-123 are based on Standards for Internal Control in the Federal Government.

[15] Project Management Institute, *A Guide to the Project Management Body of Knowledge ©* (Fourth Edition, 2008).

[16] Within TSA, the Office of Transportation Sector Network Management manages all surface transportation security issues with divisions dedicated to each surface mode of transportation, including pipeline.

[17] Exec. Order No. 13,416, 71 Fed. Reg. 71,033 (Dec. 5, 2006). The order mandates that an annex shall be completed for each surface transportation mode in support of the Transportation Systems Sector-Specific Plan.

Sector-Specific Plan,[18] and guidance on desirable characteristics for a national strategy that we developed in a previous report.[19] We also reviewed the NIPP and the 2007 Transportation Systems Sector-Specific Plan to determine the risk management framework's recommended approach to performance measurement and compared TSA's actions with that guidance. In addition, we analyzed data PSD used as an outcome measure to determine the extent of improvements in pipeline security and evaluated both the reliability of the data and its sufficiency as a measure of pipeline security outcomes. As part of this analysis, we compared two successive data collection instruments—the original instrument PSD developed in 2003 and used in conducting early CSRs with the one TSA developed in 2004, which PSD subsequently used. Later in this report we discuss concerns about the reliability of some of these data. Appendix I contains a more detailed discussion of our objectives, scope and methodology.

We conducted this performance audit from November 2008 to August 2010 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 Systems

More than 2.4 million miles of hazardous liquid and natural gas pipeline—primarily buried underground in the continental United States—run under remote and open terrain as well as densely populated areas. These pipelines are comprised of three main types:

[18] The NIPP obligates each sector to develop a sector-specific plan that, among other things, describes strategies to protect the nation's critical infrastructure and key resources under its purview. TSA developed the Transportation Systems Sector-Specific Plan, which describes the strategies to protect all modes of transportation, including pipeline.

[19] GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

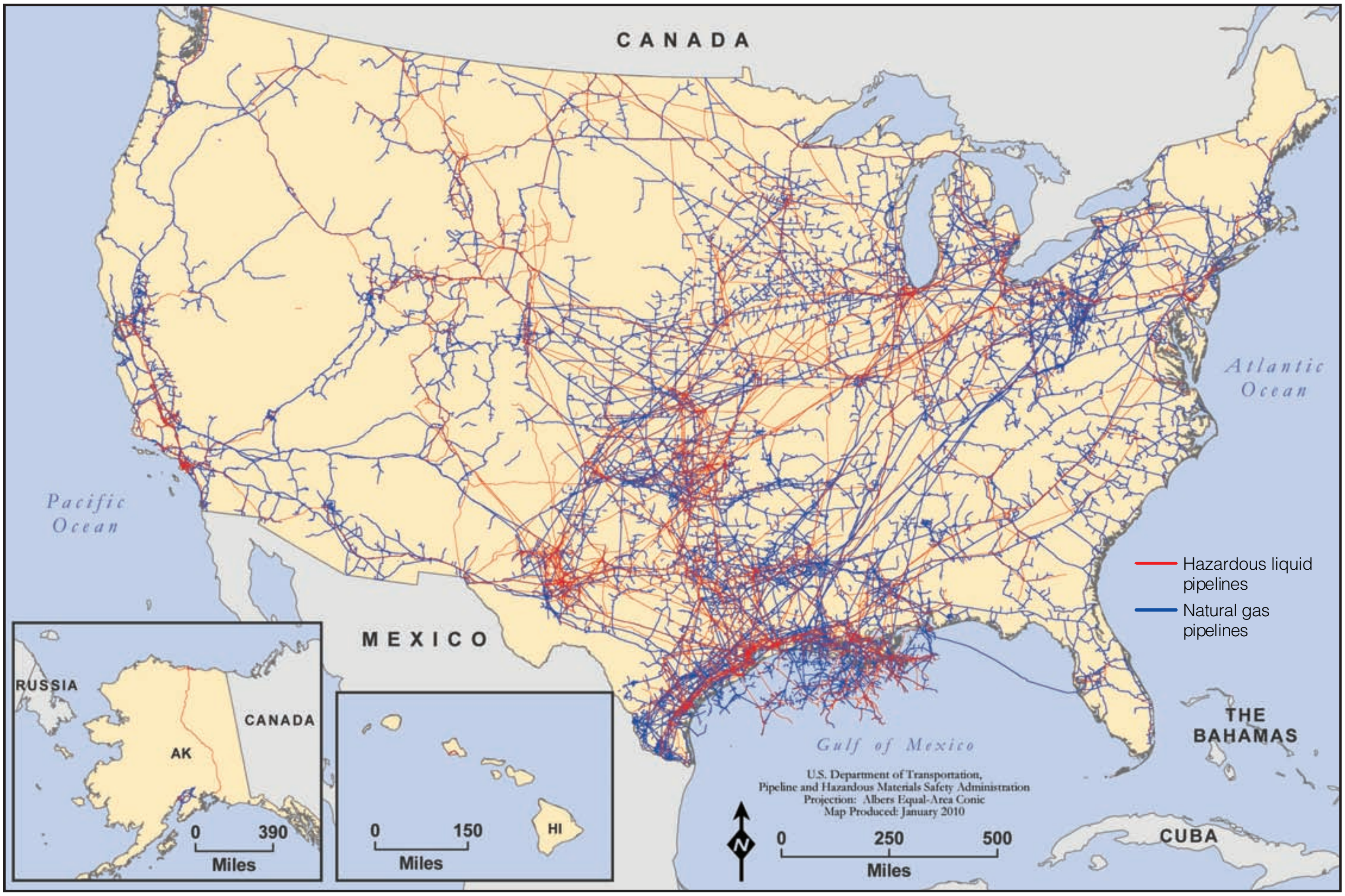
- **Hazardous liquid:** About 170,000 miles of hazardous liquid pipeline transport crude oil, diesel fuel, gasoline, jet fuel, anhydrous ammonia, and carbon dioxide.

- **Natural gas transmission and storage:** Over 320,000 miles of pipeline—mostly interstate—transport natural gas from sources to communities.

- **Natural gas distribution:** About 1.9 million miles of pipeline—mostly intrastate—transport natural gas from transmission pipelines to residential, commercial, and industrial customers.

The network of hazardous liquid and natural gas transmission pipelines in the United States can be seen in figure 1.

Figure 1: Map of Hazardous Liquid and Natural Gas Transmission Pipelines in the United States, September 28, 2009


CANADA
Atlantic Ocean
Pacific Ocean
MEXICO
Gulf of Mexico
THE BAHAMAS
CUBA
Hazardous liquid pipelines
Natural gas pipelines
RUSSIA
CANADA
AK
0
390
Miles
0
150
Miles
HI
U.S. Department of Transportation,
Pipeline and Hazardous Materials Safety Administration
Projection: Albers Equal-Area Conic
Map Produced: January 2010
N
0
250
500
Miles

Source: Department of Transportation, Pipeline and Hazardous Materials Safety Administration.

More than 3,000 pipeline companies operate the nation's pipeline systems. Pipeline systems are comprised of the pipelines themselves, which can traverse multiple states and U.S. borders with Canada and Mexico, as well as a variety of facilities, such as storage tanks, compressor stations, and control centers. Some of these facilities are considered critical and merit particular attention to security if, for example, they are important to the nation's energy infrastructure; serve installations critical to national defense; or, if attacked, have the potential for mass casualties or significant impact on public drinking water affecting a major population center. A significant disruption of pipeline service has the potential to inflict economic havoc on a region or the nation at large.

Notwithstanding the potential damage or harm that could result from an attack, the inherent design and operation of U.S. pipeline systems might reduce some of the potential impacts regarding loss of service. For one thing, the pipeline sector is generally considered to be resilient. Historically, pipeline operators have been able to quickly respond to the adverse consequences of an incident—whether it is damage from a major hurricane or a backhoe—and quickly restore pipeline service. In addition, pipeline infrastructure is versatile and includes such redundancies as parallel pipelines or looping capabilities that enable operators to mitigate potential disruptions by rerouting energy through the network.

Key Pipeline Security Stakeholder Roles and Responsibilities

Protecting the nation's pipeline systems is a responsibility shared primarily by the federal government and private industry. Since the terrorist attacks of September 11, 2001, the role of federal agencies in securing the nation's transportation systems has continued to evolve. In response to those attacks, the federal government enacted the Aviation and Transportation Security Act of 2001, which created and conferred upon TSA broad responsibility for securing all modes of transportation, including pipeline.[20] In November 2002, the federal government enacted the Homeland Security Act, which established DHS, transferred TSA from DOT to DHS, and assigned DHS responsibility for protecting the nation from terrorism, including securing the nation's transportations systems.[21]

Within TSA, the Office of Transportation Sector Network Management (TSNM) manages all surface transportation security issues with divisions dedicated to each surface mode of transportation, including pipeline. Within TSNM, the Pipeline Security Division (PSD)—the smallest of TSNM's surface transportation divisions—has lead responsibility for the security of the nation's pipeline systems.[22] For fiscal year 2010, PSD has an authorized staffing level of 13 and a budget of about $4 million. TSA's Office of Intelligence is responsible for collecting and analyzing threat information related to the transportation network; it shares with PSD any information related to pipeline threats or suspicious incidents.

[20] Pub. L. No. 107-71, 115 Stat. 597 (2001).

[21] Pub. L. No. 107-296, 116 Stat. 2135 (2002).

[22] The Pipeline Security Division was established as a separate modal division in November 2005.

While TSA, within DHS, was given primary responsibility for pipeline security, DOT's Pipeline and Hazardous Materials Safety Administration (PHMSA) retained responsibility and authority for regulating the transportation of hazardous materials via pipeline and pipeline safety. In 2004, DHS and DOT entered into a memorandum of understanding (MOU) delineating the agencies' roles and responsibilities with respect to transportation security and recognizing DHS as having primary responsibility for security in all modes of transportation, including pipeline. In 2006, TSA and PHMSA completed an annex to the MOU further clarifying both agencies' roles. The annex identifies TSA as the lead federal entity for transportation security, including hazardous materials and pipeline security, and PHMSA as responsible for administering a national program of safety in natural gas and hazardous liquid pipeline transportation, including identifying pipeline safety concerns and developing uniform safety standards. However, pipeline security and safety are intertwined, and PSD and PHMSA coordinate on matters relating to pipeline security and protection. TSA and DOE also work together on matters where pipeline safety and security overlap and PSD and DOE worked closely on pipeline security issues, programs, and activities, such as efforts to enhance reliability and resiliency.

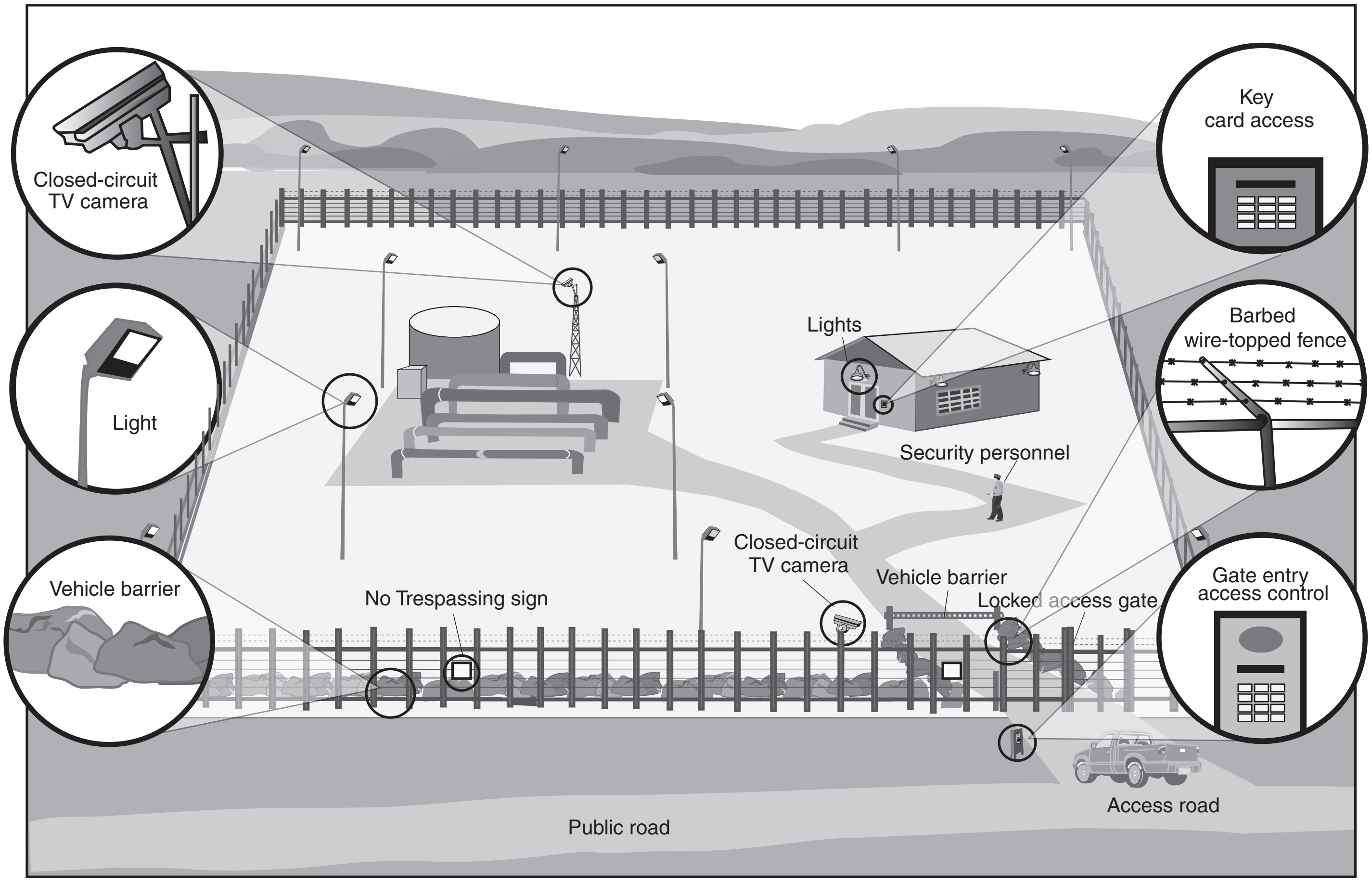
Although PSD has primary federal responsibility for pipeline security, implementation of asset-specific protective security measures remains the responsibility of pipeline operators in the private sector. Particularly since the September 11, 2001, terrorist attacks, operators' attention to security has increased and they have sought to incorporate security practices and programs into their overall business operations. Pipeline operators' interests and concerns are represented by five major trade associations with ties to the pipeline industry—the Interstate Natural Gas Association of America (INGAA), American Gas Association (AGA), American Public Gas Association (APGA), American Petroleum Institute (API), and Association of Oil Pipe Lines (AOPL). These associations have worked closely with the federal government on a variety of pipeline security-related issues.

In March 2002, API developed Security Guidelines for the Petroleum Industry and in September 2002, INGAA and AGA developed Security Guidelines for the Natural Gas Industry, which were adopted by APGA.[23]

[23] API issued a second edition of its guidelines in April 2003 and a third edition in April 2005. INGAA and AGA updated and published their guidelines internally in May 2008.

Both sets of guidelines emphasize security planning and strategies that, to varying degrees, include identifying, analyzing, and reducing vulnerabilities. Both reference some of the physical security measures that operators can take to protect their critical facilities, but provide caveats explaining the general nature of the described security practices and the importance of each operator determining the security measures that are appropriate for each facility. Figure 2 illustrates some of the physical security measures that operators may choose to employ at a critical facility.

Figure 2: Physical Security Measures a Pipeline Operator Might Employ at a Critical Facility



Sources: GAO analysis of Security Guidelines for the Petroleum Industry and Security Practices Guidelines for the Natural Gas Industry and Art Explosion (clip art).

Laws and Agency Guidance Concerning Pipeline Security

In September 2002, prior to the establishment of DHS, DOT issued voluntary guidance for pipeline operators in the form of the Pipeline Security Information Circular (the 2002 circular), which TSA later adopted. The 2002 circular, developed in collaboration with pipeline industry associations, recommended pipeline operators identify their critical facilities, develop security plans consistent with prior industry association guidance, and begin implementing appropriate security measures at critical facilities. It also outlined steps the federal government planned to take, including conducting onsite reviews of pipeline operators' security plans to determine whether the plans are consistent with security guidance published by their industry. In collaboration with industry associations, PSD developed new, draft pipeline security guidance to replace the 2002 circular. As of May 2010, PSD had not yet issued the new guidance, but it anticipates doing so sometime during 2010.

Pipeline Security Contingency Planning Guidance, also developed by DOT in 2002 and considered part of the 2002 circular, provides criteria for pipeline operators to use to identify critical facilities and establishes guidelines for protective measures for critical facilities under each threat condition corresponding to the Homeland Security Advisory System. For example, during periods of elevated threat conditions (yellow), operators should ensure, among many other things, that employees are educated on security standards and procedures; fencing, locks, camera surveillance, intruder alarms, and lighting are in place and functioning; gates and barriers are closed and locked except those needed for immediate entry and exit at critical facilities; and visitation is limited and it is confirmed that every visitor is expected and has a need to be at a critical facility. However, similar to industry guidelines, the Pipeline Security Contingency Planning Guidance also states that pipeline operators are expected to use good judgment in incorporating measures into their security plans as not all security measures are appropriate for all types of facilities.[24]

In August 2007, Congress passed the 9/11 Commission Act, which identifies the following pipeline security requirements that the Secretary of Homeland Security must implement. Some of these requirements are shared responsibilities with the Secretary of Transportation; others are to

[24] Although security measures are generally voluntary for operators of critical pipeline facilities, some operators have off-shore or port facilities that are regulated under the Maritime Transportation Security Act and are required to implement certain protective measures.

be carried out in consultation with the Secretary of Transportation.[25] Within DHS, PSD has responsibility for carrying out the following pipeline security requirements of the 9/11 Commission Act:

- Establish a program for reviewing pipeline operators' adoption of the 2002 circular, including the review of pipeline security plans and critical facility inspections.
- Develop and implement a plan for reviewing the pipeline security plans of the 100 most critical pipeline operators covered by the 2002 circular.
- Develop and implement a plan for inspecting the critical facilities of the 100 most critical pipeline operators covered by the 2002 circular.
- In conducting these reviews and inspections, use risk assessment methodologies to prioritize risks and target inspections.
- Develop security recommendations for natural gas and hazardous liquid pipelines and pipeline facilities and transmit to pipeline operators.
- If the Secretary of Homeland Security determines that regulations are appropriate, promulgate regulations and carry out necessary inspection and enforcement actions.
- Develop a pipeline security and incident recovery protocols plan and submit a report to the appropriate congressional committees. The report is to include the plan and an estimate of the private and public sector costs to implement any recommendations.

A Risk-Based Approach to Guide Pipeline Security

In recent years, we, along with Congress, the executive branch, and the 9/11 Commission, have recommended that federal agencies with homeland security responsibilities utilize a risk management approach to help ensure that finite national resources are dedicated to assets or activities considered to have the highest security priority. Homeland Security Presidential Directive 7 (HSPD-7) directed the Secretary of Homeland Security to establish uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk

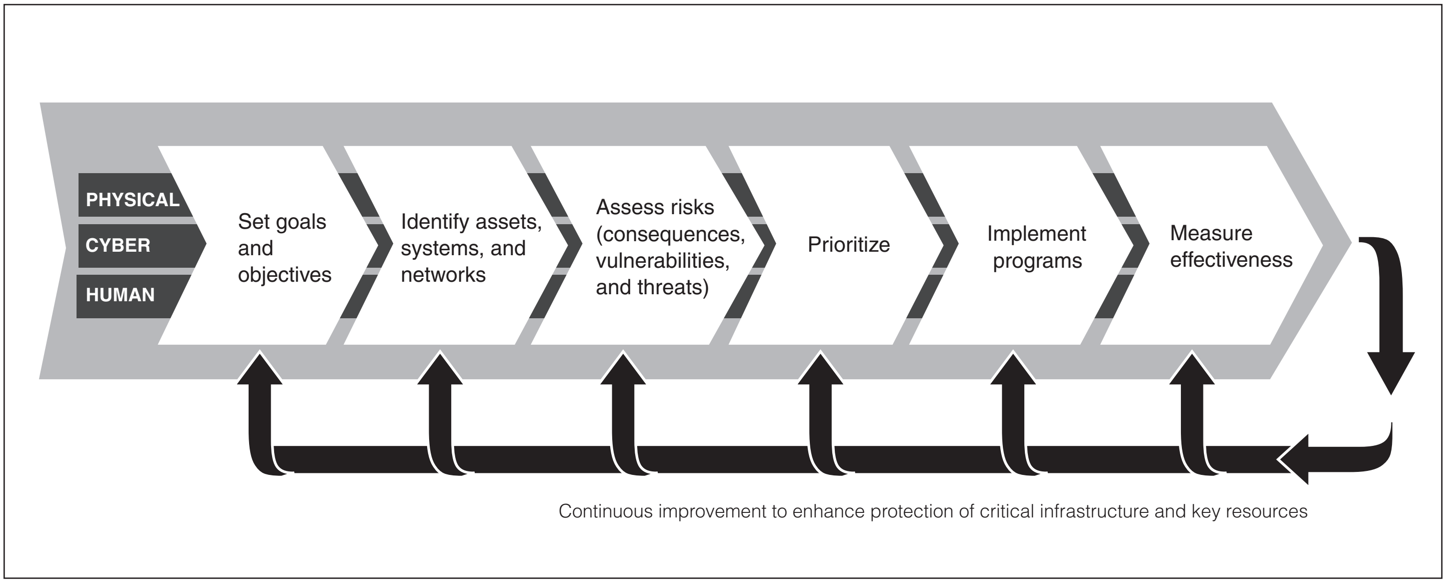
[25] Pub. L. No. 110-53, §§ 1557, 1558, 121 Stat. 266, 475-77 (2007).

management activities.[26] It also called for the Secretary to produce a comprehensive, integrated national plan for critical infrastructure and key resources protection to outline national goals, objectives, milestones, and key initiatives.

In response to HSPD-7, DHS released the NIPP in June 2006, and updated it in 2009. The NIPP created a risk-based framework for the development of sector-specific agency strategic plans. In keeping with the NIPP and as required by Executive Order 13416, TSA developed the Transportation Systems Sector-Specific Plan in 2007 to document the process to be used in carrying out the national strategic priorities outlined in the NIPP. The plan contains supporting modal implementation plans for each transportation mode, including pipeline. The Pipeline Modal Annex provides information on efforts to secure pipelines, as well as TSA's overall goals and objectives related to pipeline security. The cornerstone of the NIPP is the risk management framework that entails a continual process of managing risk through six interrelated activities, as illustrated in figure 3.

[26] Recognizing that each sector possesses its own unique characteristics and risk landscape, HSPD-7 established sector-specific agencies for each of the critical infrastructure sectors and assigned those agencies responsibility for protecting the critical infrastructure within their area of expertise. HSPD-7 established 17 sectors and DHS later added an 18th sector. The 18 sectors are: agriculture and food; defense industrial base; energy; healthcare and public health; national monuments and icons; banking and finance; water; chemical; commercial facilities; critical manufacturing; dams; emergency services; nuclear reactors, materials, and waste; information technology; communications; postal and shipping; transportation systems; and government facilities. DHS serves as the sector-specific agency for transportation systems and 10 other sectors, and designated TSA as the lead sector-specific agency for transportation, including pipeline.

Figure 3: NIPP Risk Management Framework


PHYSICAL
CYBER
HUMAN
Set goals and objectives
Identify assets, systems, and networks
Assess risks (consequences, vulnerabilities, and threats)
Prioritize
Implement programs
Measure effectiveness
Continuous improvement to enhance protection of critical infrastructure and key resources

Source: GAO, DHS.

- **Set goals and objectives:** Define specific outcomes, conditions, and end points for an effective risk management posture.

- **Identify assets, systems, and networks:** Develop an inventory of the assets, systems, and networks deemed to be critical, and collect information pertinent to risk management.

- **Assess risks:** Evaluate risk as a function of threat, vulnerability, and consequence. Once the three components of risk have been assessed for one or more given assets, systems, or networks, integrate them into a defensible model to produce risk estimates.

- **Prioritize:** Compare risk assessment results and establish priorities based on risk. Accord the highest priority in risk management activities to those assets, systems, or networks with the highest expected losses.

- **Implement programs**: Select appropriate actions or programs to reduce or manage the risk identified.

- **Measure effectiveness:** Use metrics and other evaluation tools to measure progress and assess the effectiveness of protection programs that have been implemented.

PSD Has Developed a Pipeline Risk Assessment Model, but Could Strengthen Data in the Model and Better Prioritize Security Reviews and Inspections

PSD Identified the Most Critical Pipeline Systems and Developed a Risk Model, but Some Model Components Could be Strengthened

PSD identified the 100 most critical pipeline systems in the United States,[27] consistent with the NIPP, and developed a pipeline risk assessment model to generate a risk score for those systems; however, some components of PSD's model are incomplete.[28] The NIPP calls for agencies to identify the most critical assets, systems, or networks within each sector, including the transportation sector, in order to collect information pertinent to risk management. PSD relied on each pipeline system's energy throughput to identify the most critical systems from more than 3,000 systems in the United States. It has since been focusing its risk management efforts on these 100 most critical systems, which, according to PSD officials, move 85 percent of all energy within the United States.

Once critical systems have been identified, the NIPP calls for agencies to assess risk as a function of threat, vulnerability, and consequence, and to integrate these individual assessments into a model to produce a risk estimate. It further requires that the consequence component of a risk

[27] PSD uses system annual throughput in determining pipeline system criticality, which is based on the amount of hazardous liquid or natural gas product transported through a pipeline in 1 year (i.e., annual throughput). PSD officials told us they purchase a database containing annual pipeline throughput information to determine the 100 most critical pipeline systems and contact pipeline operators to verify information if needed. The 100 most critical systems can shift from year to year. For example, a system might be among the 100 most critical systems one year, but not the next, due to changes that affect each system's throughput. Changes that can affect an operator's position or even presence among the 100 most critical systems include increasing or decreasing annual throughput, going out of business, or selling or purchasing parts or all of a pipeline system.

[28] DHS defines a risk score as a numerical result of a semiquantitative risk assessment methodology and is a numerical representation that gauges the combination of threat, vulnerability, and consequence at a specific moment.

assessment take into account the impact that an event or incident would have on the economy and public health and safety, among other things. PSD was the first of TSA's surface transportation modes to develop a risk assessment model that combines all three components of risk—threat, vulnerability, and consequence—to generate a risk score. PSD's pipeline risk assessment model generates a risk score for each of the 100 most critical systems and ranks them according to risk.[29] PSD holds the threat score constant for all pipeline systems and uses the results of its Corporate Security Reviews (CSR) in its vulnerability component. However, its consequence component is incomplete in that it accounts for economic impact, but not the impact on public health and safety. The following provides more information on the assessments or information for the threat, vulnerability, and consequence data that PSD uses in its risk assessment model.

- **Threat:** In the case of terrorist attacks, the NIPP calls for the threat component of the assessment to be calculated based on the likelihood of the intent and capability of a terrorist attack on a particular asset, system, or network. However, if threat likelihoods cannot be estimated, an agency can use conditional risk values based on vulnerability and consequence. TSA's Office of Intelligence develops Pipeline Threat Assessments and, according to officials from that office, the approach they use to assess threat is consistent across transportation modes. They further explained that because they have no actionable intelligence for specific pipeline systems, they can not develop likelihood estimates.[30] As such, PSD holds threat constant in its model and bases each pipeline system's risk score on vulnerability and consequence. Office of Intelligence officials explained that if they were to receive intelligence regarding a credible threat to a specific pipeline system, they would work with PSD officials to adjust the threat level for that system in PSD's risk assessment model.

- **Vulnerability:** According to the NIPP, agencies are responsible for ensuring that vulnerability assessments are performed within their sector in order to identify areas of weakness within a system under review. PSD uses the results of the CSRs it conducts on each of the most critical pipeline systems as the basis for the vulnerability

[29] PSD calls its risk assessment model the Pipeline Relative Risk Ranking Tool.

[30] The Office of Intelligence also disseminates additional threat and suspicious incident information related to the pipeline sector to key federal and nonfederal stakeholders, as needed.

component in its risk assessment model. PSD uses a CSR protocol (i.e., a questionnaire that guides the CSR interview) to collect information on an operator's security planning and management practices for a given pipeline system, and calculates a CSR score by tallying points associated with responses to each of 73 standard questions in the protocol.[31] Using the CSR score, PSD determines a pipeline system's vulnerability by calculating the difference or "gap" between a total possible score of 100 and an operator's CSR score. PSD uses this gap, known as the "vulnerability gap," as the basis for the vulnerability component in its risk assessment model. Using CSRs as vulnerability assessments is consistent with the approach taken by other surface transportation modes, such as freight rail and highway infrastructure, on which we have previously reported.[32]

- **Consequence:** According to the NIPP, consequence assessments should measure key effects on the well being of the nation. This includes the negative consequences on the economy, public health and safety, and the environment, as well as the functioning of government that can be expected if an asset, system, or network is damaged, destroyed, or disrupted by a terrorist attack. Within its risk assessment model, PSD uses the annual energy throughput of a pipeline system to help measure the possible adverse economic impact of a terrorist attack or other event on a pipeline system, but does not take into account other possible adverse impacts, such as on public health and safety. According to PSD officials, because the major consequence of an attack on a pipeline would be the loss of energy, annual energy throughput provides a good measure of this expected loss. However, the consequences of some potential attacks might not be limited to the economy. For example, under some circumstances, an attack on a critical pipeline facility located near a waterway has the potential to significantly contaminate drinking water or, if located in a highly populated area, could result in significant casualties.

[31] "Standard" questions refer to the ones that PSD scores and uses in calculating the CSR score. The CSR protocol includes five additional questions that are not scored, such as questions on the operator's view of the threat to the pipeline industry and how cost affected the operator's ability to implement security enhancements.

[32] GAO, *Highway Infrastructure: Federal Efforts to Strengthen Security Should Be Better Coordinated and Targeted on the Nation's Most Critical Highway Infrastructure*, GAO-09-57 (Washington, D.C.: January 30, 2009); *Commercial Vehicle Security: Risk-Based Approach Needed to Secure the Commercial Vehicle Sector*, GAO-09-85 (Washington, D.C.: February 27, 2009); and *Freight Rail Security: Actions Have Been Taken to Enhance Security, but the Federal Strategy Can Be Strengthened and Security Efforts Better Monitored*, GAO-09-243 (Washington, D.C.: April 21, 2009).

PSD officials explained that the pipeline risk assessment model is in the early stages of development and they intend to improve it over time by incorporating additional data. PSD has sponsored or conducted assessments and collected information on pipeline systems, some of which could be used to enhance individual components of its model. For example, through its Critical Facility Inspection (CFI) Program, PSD has collected information on critical facilities, such as the number of facilities per system, and officials say they plan to eventually use these data in their risk estimates. PSD officials explained that the number of critical facilities can be an indicator of a system's vulnerability—that is, the more critical facilities a system has, the more vulnerable the system. Thus, incorporating this information into the vulnerability component of PSD's risk assessment model and including it in the risk estimate could enhance the model. In addition, including information that might be available from other sources, such as the number of miles of pipeline that run through a high-consequence, or highly populated, area could also enhance the consequence component of the model. PSD officials noted that such data could be a good measure of the effects on public health and safety. However, the officials explained that with a small staff, they have not had time to make any specific enhancements to the model.

PSD officials also agreed that adding other information that could be available in the future might further improve its model. For example, PSD and DOE sponsored regional gas pipeline studies that include information that could be used to improve the consequence component of the model. These studies use computer-based modeling to evaluate the impact of a major natural gas pipeline disruption. PSD officials told us they would like to incorporate such information into the consequence component of its risk model, but adding such information for natural gas pipelines without adding comparable information for hazardous liquid pipelines would skew its risk ranking of the most critical pipeline systems. PSD officials told us in May 2010 that they had secured funds to contract for a similar assessment of the hazardous liquid pipeline market and expect the work to begin later in fiscal year 2010. They also said they plan to use the results of their CFIs to enhance the vulnerability components of the risk model; however, they will need to wait until they complete inspections of all critical facilities associated with the 100 most critical pipeline systems. The officials told us they expect to complete these inspections by the end of 2011.

Although PSD officials said they would like to add more information to their pipeline risk assessment model and have included placeholders in the model for incorporating other vulnerability and consequence factors when additional information is known, they have not established time frames or milestones (i.e., a schedule of actions needed to achieve goals) for doing this. Standard practices for program management call for establishing time frames and milestones as part of a plan to ensure that results are achieved.[33] Developing a plan that includes time frames and milestones could help PSD accomplish its goal of improving the data in its risk assessment model. By including additional information in its risk model—some that exists and some that should be available in the future—PSD could improve its risk assessment of the most critical pipeline systems and better assure it has the information it needs to guide decisions, including allocating resources to the highest risk pipeline systems. Table 1 summarizes all of TSA's assessment activities related to the three individual components of risk for the pipeline industry, and identifies which ones PSD includes in the data it inputs into its risk assessment model.[34]

[33] The Project Management Institute, *The Standard for Program Management* © (2006).

[34] DHS's Office of Infrastructure Protection also conducts vulnerability assessments on some pipeline facilities. However, because these assessments are conducted at the facility level rather than the system level, PSD cannot use these assessments in its risk assessment model, which focuses on the system level.

Table 1: TSA Pipeline Security Assessment Activities Since 2003

			Risk component addressed			Included in pipeline risk assessment model
Entity	**Time frame**	**Description**	**Threat**	**Vulnerability**	**Consequence**	
TSA Office of Intelligence	Annually	**Annual Threat Assessments:** TSA's Office of Intelligence provides an overview of threats—including key actors and possible attack tactics and targets—to pipeline systems. The assessments include incidents of interest and suspicious activities targeting pipeline systems in the United States and overseas.	X			**Yes.** PSD uses this for the threat component of the risk model.
TSA Pipeline Security Division	Ongoing since 2003	**Corporate Security Reviews (CSR):** PSD conducts CSRs to assess pipeline security plans at the 100 most critical pipeline systems in the United States. The intent of these on-site reviews of pipeline companies is to develop firsthand knowledge of security planning, establish communication with key pipeline security personnel, and identify and share good security practices.		X	X[a]	**Yes.** PSD uses CSRs for the vulnerability component of the risk model.
TSA Pipeline Security Division	Ongoing since Nov. 2008	**Critical Facility Inspections (CFI)**: PSD, with the help of a contractor, conducts in-depth inspections of all the critical facilities of the 100 most critical pipeline systems in the United States.		X	X	**No**. PSD collects the number of critical facilities per system, which could be used to enhance the risk model. PSD also collects consequence information for each system that could be used once PSD completes all inspections.
TSA Pipeline Security Division and Natural Resources Canada	2004-2007	**Pipeline-Cross-Border Vulnerability Assessments Program**: U.S. and Canadian teams assess pipeline operations, control systems, interdependencies, and assault planning in critical cross-border infrastructure.		X	X	**No**. PSD cannot use this in its risk model because it involves only a few of the 100 most critical pipeline systems.

			Risk component addressed			Included in pipeline risk assessment model
Entity	Time frame	Description	Threat	Vulnerability	Consequence	
TSA Pipeline Security Division – initiated by DOE	2003-2008	**Regional Gas Pipeline Studies**: PSD, in coordination with DOE, sponsored a series of studies using computer-based modeling, to evaluate the impact of a major pipeline disruption.[b]			X	**No**. PSD cannot use this information until a comparable study for hazardous liquid pipelines is completed.
TSA Pipeline Security Division	Ongoing	**Cued Assessments:** When intelligence activities indicate that a pipeline operator has been under possible terrorist surveillance, PSD works with the operator to conduct vulnerability and consequence assessments to determine the existing state of security and gaps that need to be addressed. After these assessments, PSD makes recommendations on how to close the security gaps.		X	X	**No.** PSD cannot use this information because such assessments are isolated. Thus, PSD does not have such information for all of the 100 most critical pipeline systems.

Source: GAO and PSD.

[a] PSD collects consequence information during a CSR, but does not conduct a consequence assessment.

[b] INGAA and AGA funded the first in this series of studies.

PSD Could Better Prioritize Its Reviews and Inspections of Critical Pipeline Systems Based on Risk

PSD's CSR procedures call for scheduling CSRs based primarily on a pipeline system's risk ranking as determined by its risk assessment model; however, we found a weak statistical correlation between a system's risk ranking and the time elapsed between the first and subsequent CSR for a pipeline system.[35] This suggests that a system's risk ranking was not the primary consideration in scheduling these reviews. For the pipeline systems included in PSD's risk assessment model dated May 2010, PSD had conducted 54 initial CSRs of pipeline operators who operate the 100 most critical systems, and 27 second CSRs of those operating 65 of the

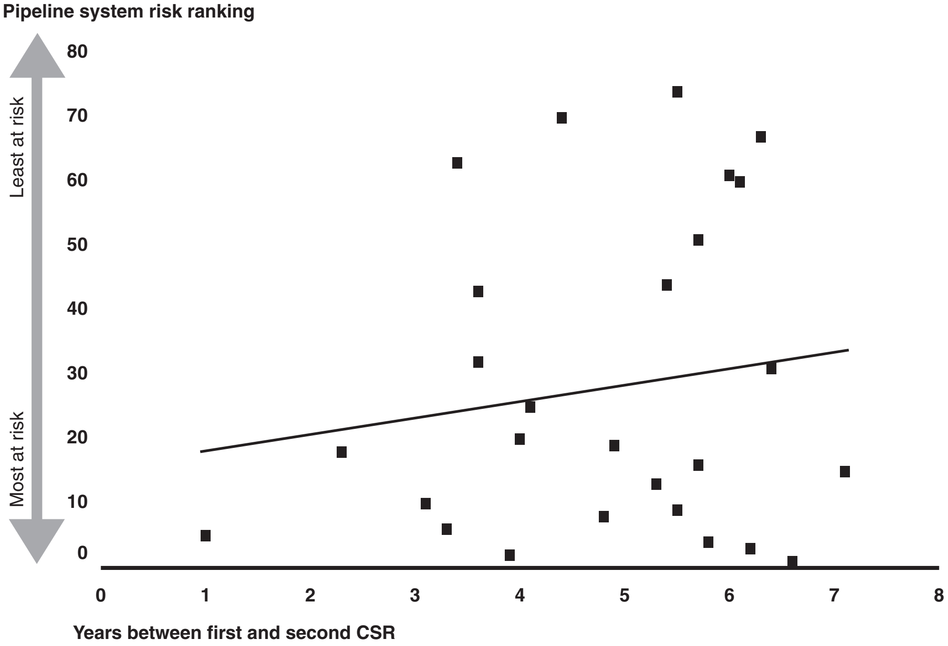
[35] We calculated a simple correlation coefficient to measure the strength and direction of the linear relationship between systems' risk rankings and the time elapsed between PSD's first and subsequent CSRs for the pipeline systems that had two CSRs. This resulted in a correlation coefficient score of 0.2, which indicates a weak correlation. The magnitude of the correlation coefficient determines the strength of the correlation. A perfect correlation equals 1 and no correlation equals 0.

most critical pipeline systems.[36] Figure 4 illustrates the weak correlation we found between risk ranking and time between reviews for the 27 operators with which PSD conducted a second CSR, as denoted by data points that are not clustered near or on the line of best fit.[37] If a stronger correlation existed between these variables, the data points would be clustered closer to the line of best fit.

[36] PSD conducts CSRs with operators of the 100 most critical pipeline systems. If an operator owns or operates more than one system among the 100 that are most critical, and uses the same corporate security plan for all its systems, PSD conducts a single CSR for that operator. As a result, PSD did not need to conduct 100 CSRs to complete CSRs for the 100 most critical pipeline systems.

[37] The line of best fit is found by using the least squares method, which involves finding the minimum of the sum of the squares of the vertical distances of each data point from the proposed line. It is often useful to attempt to represent data with the equation of a straight line in order to predict values that may not be displayed on a scatter plot. The slope of the line of best fit generally does not reflect the magnitude of the correlation.

Figure 4: Correlation Between a Pipeline System's Risk Ranking and the Time Elapsed from the First to the Second CSR, as of May 2010



Source: GAO analysis of PSD data.

Notes: n=27.

In 27 cases, PSD conducted two CSRs for the same operator. These CSRs were conducted from April 2003 through May 2010. Because some pipeline operators operate more than one system and a CSR usually covers all the systems operated by a given operator, these 27 CSRs covered a total of 65 of the 100 most critical pipeline systems.

According to CSR procedures, using a pipeline system's risk ranking when scheduling CSRs allows PSD to consider the importance of the system to the nation's transportation infrastructure and the likelihood that the system could be attacked. Similarly, according to the NIPP, the highest priority in risk management efforts should be accorded to those systems with the highest expected losses. In addition, the 9/11 Commission Act requires that risk assessment methodologies be used to prioritize risk and to target inspection actions to the highest risk pipeline assets. According to PSD officials, a pipeline system's relative risk ranking is the primary factor driving their decision of when to schedule a subsequent CSR, however, other factors, such as geographic proximity, also affect the decision. For example, in some cases PSD officials schedule a CSR for a lower risk-ranked system that might be located in the same geographic area as a higher risk-ranked system to be efficient and reduce travel time and costs.

We also found considerable variation in the time elapsed before PSD returned to conduct a second CSR. For example, our analysis of the data in PSD's risk assessment model showed:

- Within the 15 highest risk-ranked pipeline systems, the time between the first and second CSR ranged from 1 to 7 years.[38]
- For all pipeline systems, the average time elapsed between a first and second CSR was 4.8 years, regardless of the system's risk ranking.[39]
- For 5 systems that rank in the top 15 in terms of risk, approximately 6 years elapsed between a first and second CSR—more than the average time for all systems.

PSD officials stated that although the time elapsed between a first and second CSR might be longer than average for some of the highest risk pipelines, this does not mean that PSD has not been focusing its attention on these operators. For example, in one of these cases, the officials explained they spent 6 weeks in 2009 inspecting dozens of critical facilities belonging to this operator through the CFI program, met with the company president to discuss the need for security improvements, and had other contacts with the operator. However, even after accounting for PSD inspecting one or more of an operator's critical facilities before conducting a second CSR, we still found a weak relationship between a pipeline system's risk ranking and the time elapsed between that system's first and subsequent CSR.[40]

[38] As of May 2010, PSD had conducted second CSRs for 9 of the top 15 highest risk-ranked systems. PSD conducted first CSRs for the other 6 systems in 2006 or later.

[39] Because some CSRs cover multiple systems (since some operators operate more than one system), we accounted for one system, or one CSR, per operator in our calculations.

[40] We calculated a regression equation to see the extent to which values of the two independent variables—(1) a system's risk ranking and (2) whether PSD had inspected any critical facilities belonging to a system's operator—were associated with values of the dependent variable—i.e., the time elapsed between a first and second CSR. We found little variation in the time elapsed between CSRs that could be explained by the two independent variables. Although PSD officials might have had contact with pipeline operators through other means, we could not quantify other forms of contact and, therefore, could not include them in the analysis.

The NIPP calls for systems that are considered to have the highest expected losses if damaged, disrupted, or destroyed, to receive more scrutiny. Furthermore, PSD's CSR procedures state that the CSR program should consider a pipeline system's risk level as one of the most crucial factors when scheduling CSRs and PSD officials told us they consider a system's risk to be the primary factor in these decisions. However, PSD has not clearly stated in its CSR procedures that risk should be the primary criteria in scheduling CSRs, nor has it documented a methodology addressing how it is to balance other practical considerations, such as travel efficiencies, with its consideration of risk. Doing so could help PSD ensure it prioritizes its oversight of pipeline systems that are most at risk.

Similarly, PSD has no documented procedures or methodology for using a system's risk ranking when scheduling CFIs. According to PSD officials, when they began the CFI program in November 2008, their primary consideration in scheduling CFIs was to do so in a manner that would allow them to complete a large number of inspections as soon as possible. For example, if 10 critical facilities were located close enough to each other to complete all 10 in 1 week, PSD would schedule those inspections and leave the inspections of more geographically dispersed critical facilities for a later time. The officials further explained that because inspecting outdoor space is critical to a CFI, they also consider weather when scheduling inspections (i.e., scheduling cold weather locations in warmer months). However, the NIPP calls for according the highest priority in risk management efforts to those systems with the highest expected losses. Furthermore, the 9/11 Commission Act requires that risk assessment methodologies be used to prioritize risk and to target inspections to the highest risk pipeline assets. Documenting a methodology for scheduling CFIs and including a pipeline system's risk ranking as the primary criteria while recognizing other considerations that can affect scheduling could help PSD ensure it prioritizes its oversight of pipeline systems that are most at risk.

We identified almost no statistical correlation between the order in which PSD conducted critical facility inspections and the risk ranking of the pipeline system containing those facilities.[41] For example, PSD did not inspect any of the critical facilities of three of the highest risk-ranked systems until early 2010, although it had conducted CFIs of some of the lowest risk-ranked systems in the previous year. PSD's oversight of the critical facilities belonging to the most at-risk pipeline systems could be better prioritized by scheduling inspections of facilities based on their system's risk ranking.

PSD Has Taken Actions to Implement Agency Guidance and 9/11 Commission Act Requirements, but Lacks a System for Following Up on Its Recommendations to Operators

PSD Established a Program for Reviewing Pipeline Security Plans

PSD established an on-site CSR program in April 2003 that has been evolving in response to, and consistent with, agency guidance—specifically, DOT's September 2002 Pipeline Security Information Circular (the 2002 circular)—and the 9/11 Commission Act. PSD undertook CSRs to determine the state of security within the pipeline industry and enhance the level of security planning and preparedness throughout the industry. The 2002 circular outlines voluntary actions that pipeline operators should take and describes actions the federal government plans to take to

[41] As of April 2010, 64 systems included in PSD's risk assessment model had at least one critical facility, according to information operators reported, and PSD had inspected at least one critical facility of 43 of these 64 systems. We calculated a simple correlation coefficient to measure the strength and direction of the linear relationship between the systems' risk rankings and when (i.e., the order in which) PSD conducted the first critical facility inspection of that system. This resulted in a correlation coefficient score of 0.03, which indicates almost no correlation.

improve pipeline security.[42] It gives operators some discretion to determine which security measures are appropriate for each of their critical facilities and provides the federal government with broad guidance and, thus, some flexibility, in carrying out its reviews. According to the 2002 circular, pipeline operators should take the following actions:

- Identify critical facilities.[43]

- Develop a corporate security plan that is consistent with voluntary security guidance published by the pipeline industry.[44]

- Begin to implement appropriate security measures for the critical facilities.

In addition, the 2002 circular describes the following actions the federal government planned to take:

- Review pipeline operators' security plans on site.

- Determine whether operators' security plans are consistent with security guidance published by their industry.

- Conduct spot checks of selected critical facilities in the field to verify operators are implementing their security plans as written.

- Work with operators to correct security deficiencies.

CSRs emphasize the importance of pipeline operators' management practices in prevention, protection, and response to threats. They focus on pipeline operators' security plans and how operators manage their security programs, and include recommendations to operators for application in routine operational practices and during heightened alert levels. These

[42] Although these security measures are generally voluntary for operators of critical pipeline facilities, some operators have off-shore or port facilities that are regulated under the Maritime Transportation Security Act and are required to implement certain protective measures.

[43] If an operator considers none of its facilities to be critical, the operator should document the basis for this conclusion.

[44] INGAA and AGA published security guidelines for the natural gas industry, which were adopted by APGA; API published security guidelines for the petroleum industry.

reviews are also intended to provide PSD a means to establish and maintain relationships with pipeline operators' key security personnel.

CSRs include detailed interviews with the pipeline operators' security personnel—typically at operators' corporate headquarters; spot checks of selected facilities; reviews of security plans and related documents; and PSD feedback, including recommendations specific to the operator.[45] A CSR team, comprised of PSD officials, conducts the interview using a CSR protocol that PSD developed based on the 2002 circular and industry guidance.[46] The protocol includes 73 standard questions divided into 11 areas that include vulnerability assessments, credentialing, security training, cyber security,[47] and physical security.[48] According to the PSD General Manager, the CSR process gives PSD some confidence that operators are doing what their corporate security plans say. Further, he expects that operators who do well on a CSR generally have reasonably good security measures in place at their critical facilities. However, he noted that it is difficult to be certain of the physical security measures in place at critical facilities without conducting full inspections.

When the 9/11 Commission Act was enacted in August 2007, it reinforced the CSR program that PSD had underway by specifically requiring reviews of pipeline operators' security plans for the 100 most critical pipeline

[45] PSD officials explained they began conducting inspections of critical facilities as part of a new program in November 2008 and curtailed CSR spot checks of selected facilities at that time.

[46] We compared industry guidance to the CSR protocol and found that the protocol generally allows PSD to determine whether a pipeline operator's corporate security plan is consistent with industry guidance.

[47] CSRs include questions pertaining to cyber security, but according to PSD officials, they do not involve in-depth inspections or assessment of an operator's cyber security system and its vulnerabilities because PSD does not possess this expertise. They explained that other federal component agencies, such as DHS's National Cyber Security Division, have this expertise, and pipeline operators typically have in-house expertise or contract for it.

[48] The CSR protocol is divided into the following 11 functional areas: threat assessment, vulnerability assessment, security planning, credentialing, secure areas, critical infrastructure, physical security, cyber security, security training, communications, and exercises.

systems.[49] Within the first 5 years of conducting CSRs, PSD had reviewed the 100 most critical systems and had begun a second round of CSRs. As of May 2010, it had completed 103 CSRs covering more than 125 pipeline systems, including 76 first-time CSRs and 27 second-time CSRs.[50] According to PSD officials, CSRs have shown that pipeline operators are generally implementing voluntary security measures and that second CSRs have indicated that operators are generally improving their security posture.

We observed a CSR team conducting four CSRs from August through October 2009. These represented a first CSR for two of the operators and a second CSR for the remaining two operators—both of which had a first CSR in 2004. The CSR team followed the same general process for all four CSRs, asked all the questions in the CSR protocol, and conducted the CSRs in a manner consistent with CSR program goals (i.e., emphasizing the importance of security management practices, establishing working relationships with pipeline security personnel, and identifying and sharing knowledge of best practices).

The CSR team found that the security posture of these four operators varied considerably. As part of each CSR, the team identified security practices the operators were implementing well, but also made recommendations regarding areas for improvement, tailored to each operator and based on the results of each review. For the four CSRs we observed, the CSR team made a total of 32 recommendations, ranging from 3 recommendations to one operator and 17 recommendations to another. For example, officials recommended that one operator conduct vulnerability assessments for its critical facilities, another operator should issue identification cards to contractors, and a third should add certain emergency contact information to its security plan and add its new headquarters to its list of critical facilities.

[49] The 9/11 Commission Act requires DHS to establish a program for reviewing pipeline operator adoption of the recommendations of the 2002 circular, including the review of pipeline security plans, and requires DHS to develop and implement a plan to review the pipeline security plans of the 100 most critical pipeline operators covered by the 2002 circular. Pub. L. No. 110-53, § 1557(a), (b), 121 Stat. 266, 475 (2007).

[50] Because PSD updates the 100 most critical systems annually using pipeline system energy throughput data, which is revised annually, PSD has conducted CSRs of operators whose systems once were, but may no longer be, on the most critical list. Also, as noted earlier, because some pipeline operators own or operate more than one of the 100 most critical systems, PSD did not need to conduct 100 CSRs to cover all 100 most critical systems.

PSD Established a Program for Inspecting Critical Facilities of the Most Critical Pipeline Systems

PSD established the CFI program to conduct inspections of all the critical facilities of the 100 most critical pipeline systems, as required by the 9/11 Commission Act.[51] According to PSD officials, the purpose of the CFIs is to take a one-time snapshot of each critical facility's security posture—that is, to collect information on each critical facility's security measures and equipment. PSD relied on pipeline operators to identify their own critical facilities using criteria contained in the 2002 circular. As of May 2010, operators of the 100 most critical systems had notified PSD of a total of 373 critical facilities; however, PSD officials explained that this number is fluid.

PSD manages the CFI program and has contracted with a security and risk management consulting firm that focuses primarily on energy infrastructure security to help with the program's design and implementation. CFI teams (comprised of PSD staff and contractors from the consulting firm) began conducting CFIs in November 2008 and, as of May 2010, had completed 224 CFIs. Due to the time- and resource-intensive nature of these inspections, PSD officials estimated they will finish inspecting all the critical pipeline facilities operators have identified by the end of 2011. Each CFI takes roughly 4 hours and entails the following steps:

- The CFI team conducts an in-depth interview regarding the operator's security practices using a CFI protocol that covers more than 150 items.
- The CFI team conducts an on-site physical inspection of the interior and exterior of each critical facility, including the perimeter of the property. Through physical observation and some testing, the CFI team confirms that the security measures discussed during the CFI interview are actually in place.
- The CFI team shares with the operator's security personnel its observations of good security practices, areas for improvement, and security recommendations.

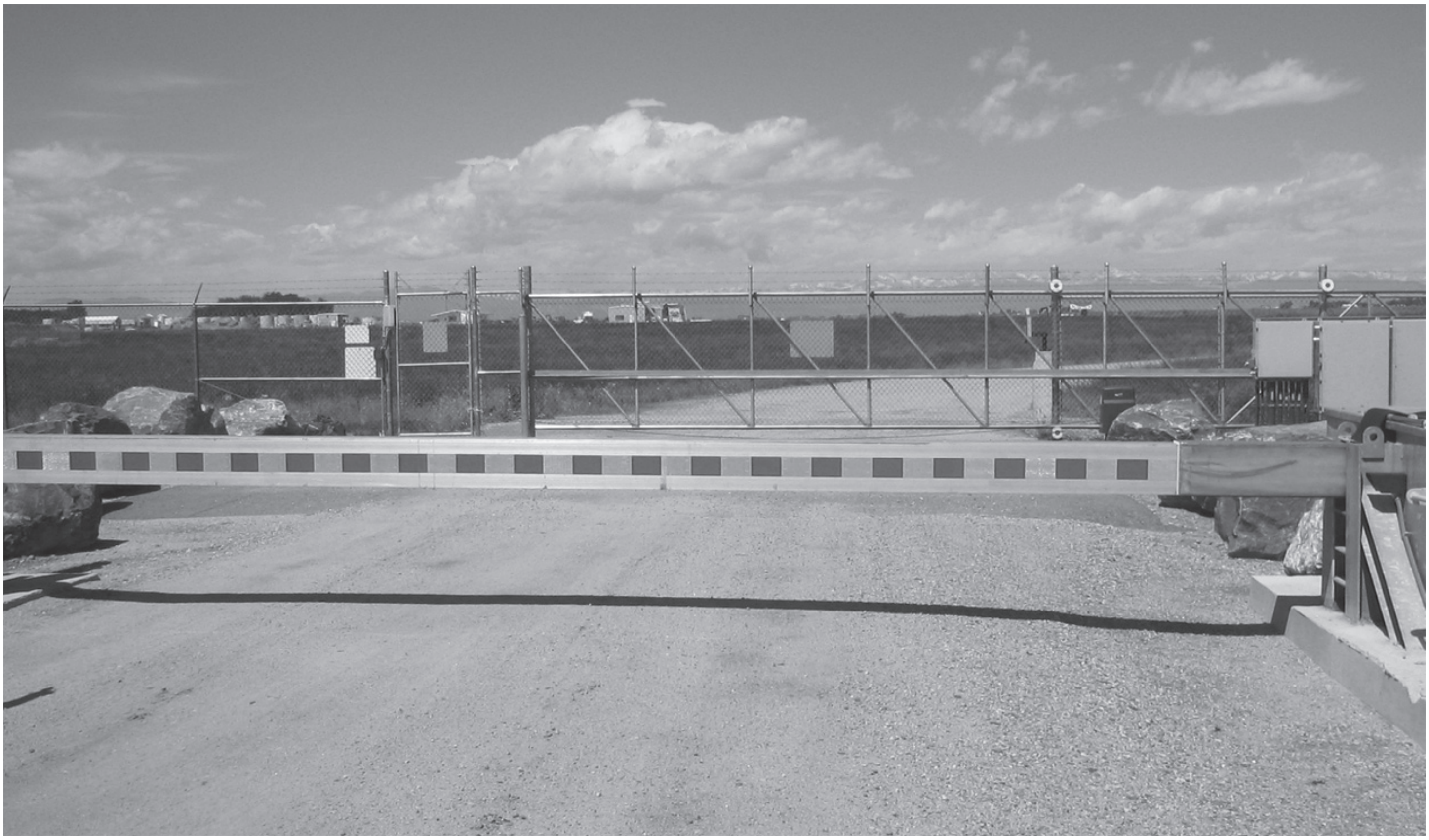
[51] The 9/11 Commission Act requires DHS to establish a program for reviewing pipeline operator adoption of the recommendations of the 2002 circular, including critical facility inspections, and requires DHS to develop and implement a plan to inspect the critical facilities of the 100 most critical pipeline operators covered by the 2002 circular. Pub. L. No. 110-53, § 1557(a), (b), 121 Stat. 266, 475 (2007).

- PSD sends the operator a final inspection report for each facility inspected, including recommendations, subsequent to the CFI.

From June through August 2009, we observed the CFI team conduct 10 CFIs involving critical facilities operated by three different pipeline operators. The CFI teams we observed followed the same general process for each inspection and asked all the questions in the CFI protocol. The security posture at these facilities varied considerably, and the CFI team's observations and recommendations varied accordingly. During each CFI, the team commended the operator for specific security practices that were in place at the facility, but also made recommendations for actions to improve security. The CFI team made a total of 88 recommendations for the 10 CFIs we observed, ranging from 4 recommendations at some facilities to 13 recommendations at others. For example, recommendations the CFI team made to one operator included overhauling the procedure for obtaining visitor badges and installing "no trespassing" signs and warnings indicating that the property is under video surveillance. Recommendations to another operator included securing all perimeter gates when not in active use, installing an access control system at the main gate that logs activity, upgrading main gate lighting, and establishing a formal key management program.

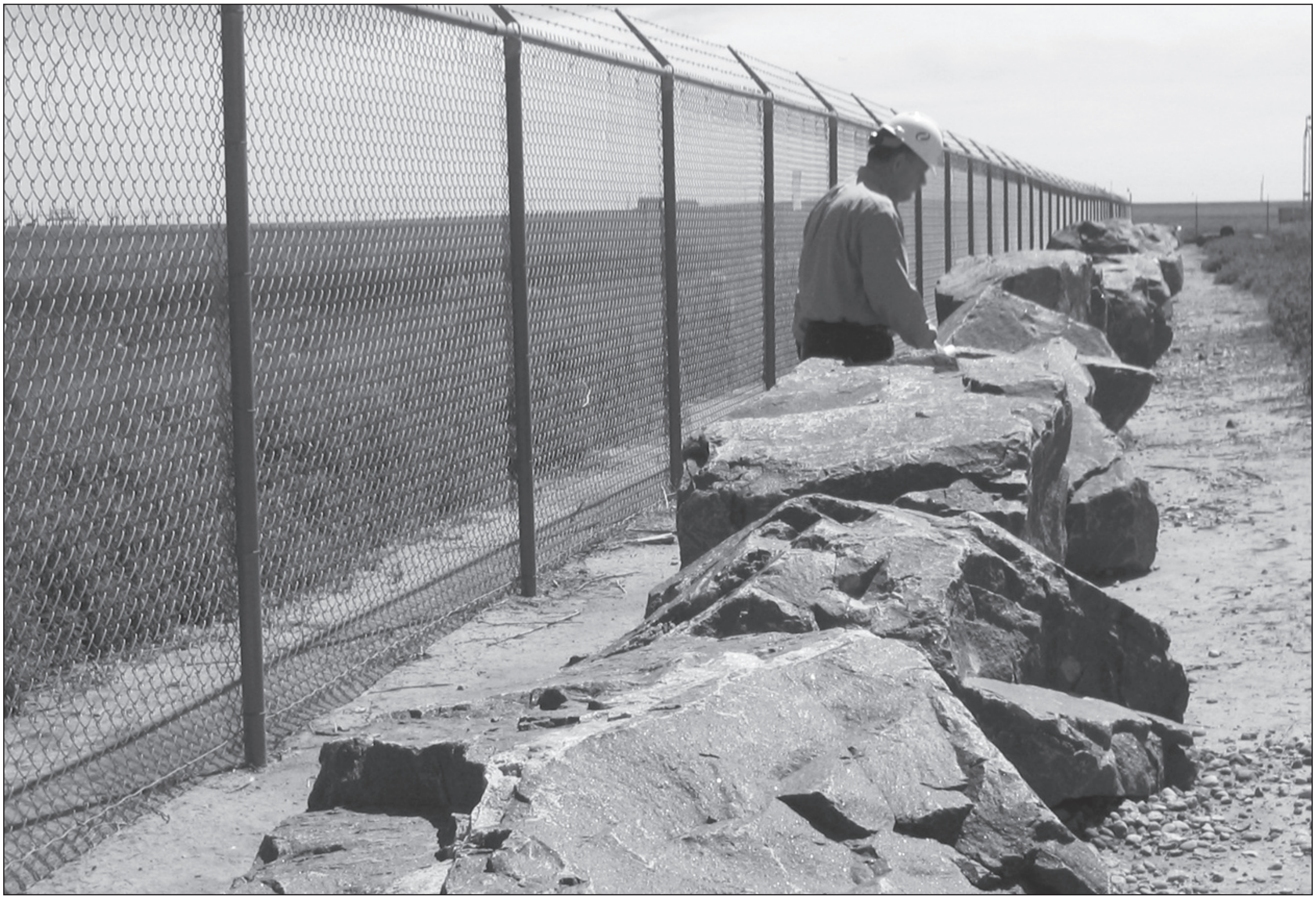
Figures 5, 6, and 7 show several of the security measures for which the CFI team commended the operator during a CFI we observed.

Figure 5: Antiterrorism Crash Barrier Gate Installed inside Fenced Perimeter of a Critical Facility



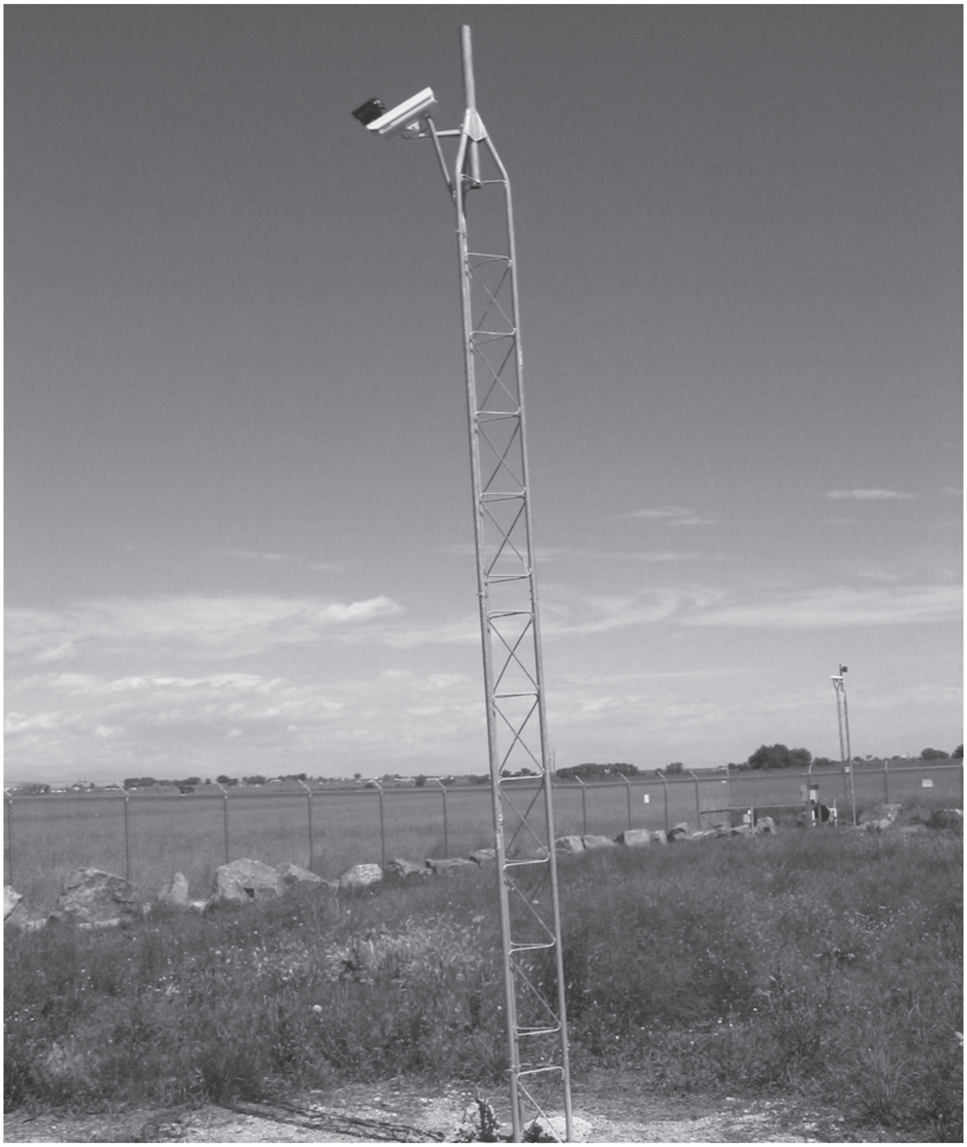
Source: GAO.

Figure 6: Boulders Installed inside Perimeter Fencing at a Critical Facility Serve as a Vehicle Barrier



Source: GAO.

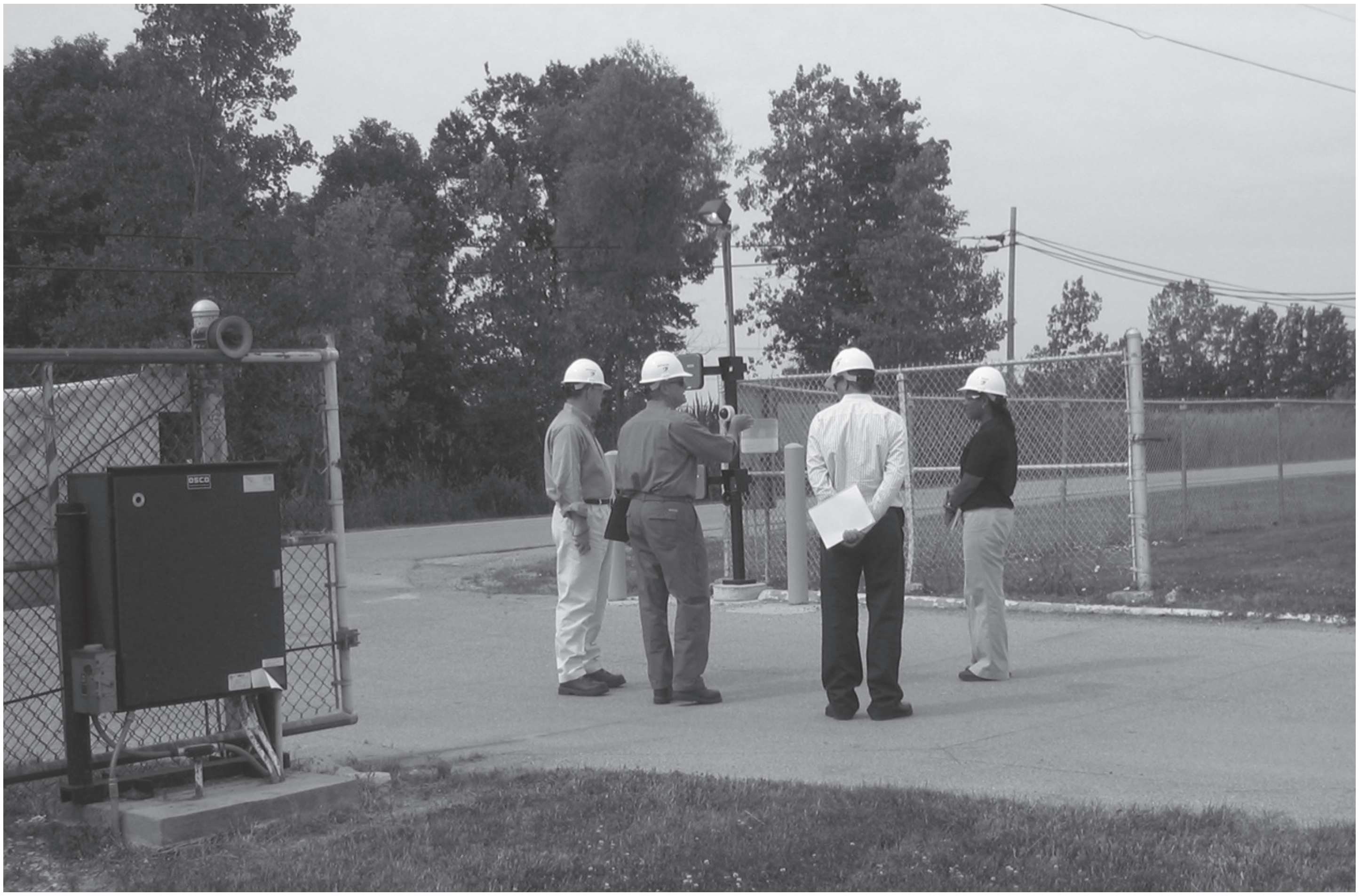
Figure 7: One of Many Closed-Circuit Television Cameras Installed at a Critical Facility



Source: GAO.

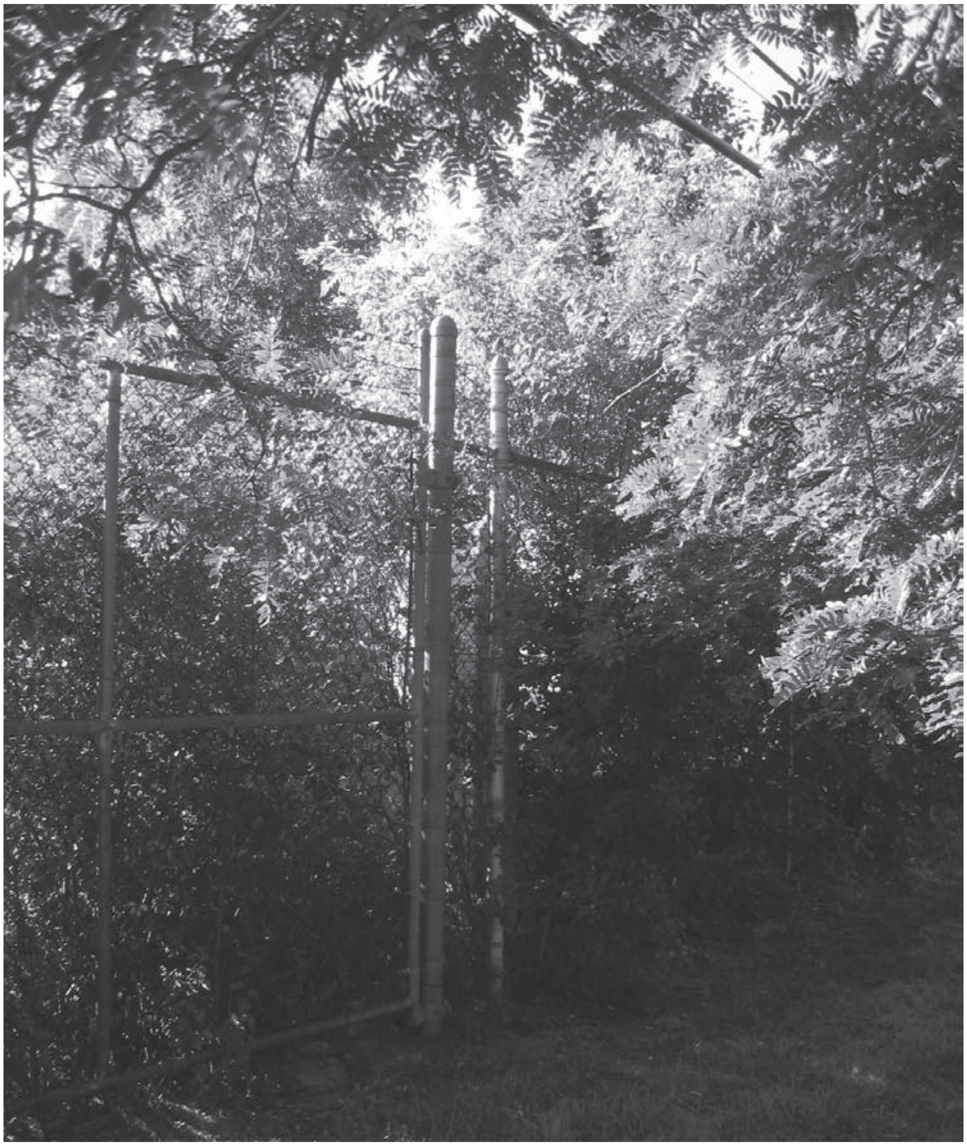
Figures 8 and 9 are photographs of two types of security lapses the CFI team identified during two other CFIs we observed. The CFI team made recommendations to the operator to address these and other security vulnerabilities.

Figure 8: CFI Team Explains That Leaving the Entry Gate of a Critical Facility Open during Business Hours Constitutes a Serious Lapse in Security



Source: GAO.

Figure 9: Excessive Vegetation Surrounding a Critical Facility Impedes the Operator's Ability to Inspect Fencing and See Possible Intruders



Source: GAO.

In addition to accompanying CFI teams on inspections, we independently observed the exterior of 10 critical facilities operated by six different pipeline operators. Based on what we could observe at these facilities from outside the property perimeters, we saw variation in the physical security measures that these operators appeared to have in place—not dissimilar to what we observed when we accompanied CFI teams on their inspections.

In contrast to CSRs, which look at pipeline operators' corporate security plans and security management, CFIs, when all are completed, are to yield information on security measures in place at every individual critical pipeline facility that operators have identified. According to PSD's General Manager, the CFI program fills a gap that existed in the CSR program by providing PSD the ability to develop first-hand knowledge of security measures in place at critical pipeline sites. As designed, the program provides PSD with a single point-in-time snapshot of the security posture of each critical facility. PSD officials explained that the CSR and CFI programs are complementary and that the CSRs' focus on management practices and the CFIs' focus on security measures in place at critical facilities provide PSD with needed information and are both important. They further stated that, because of its value, they are discussing ways to continue the CFI program after they complete all the inspections if resources are available. Options discussed include repeating the full set of CFIs after inspections of the critical facilities of the 100 most critical systems are completed; expanding inspections beyond these 100 systems, including toxic inhalation hazard pipeline systems; and enhancing CSRs to incorporate more thorough inspections of critical facilities.[52]

PSD Does Not Routinely Follow Up on Recommendations to Pipeline Operators

PSD does not routinely transmit its CSR recommendations in writing to pipeline operators, nor does it have a database of the CSR or CFI recommendations it makes or a process to routinely follow up on pipeline operators' implementation of those recommendations. After each CSR, PSD officials document review findings and the recommendations they make in an internal PSD report and provide oral recommendations aimed at enhancing that operator's security planning and preparedness to the pipeline operator's security personnel and sometimes management. However, PSD officials said they do not communicate these recommendations to the operator in writing as a matter of practice, but will transmit them in writing if an operator asks. Of the four CSRs we

[52] Toxic inhalation hazard pipelines, such as those transporting anhydrous ammonia and chlorine gas, are among the most dangerous. These pipelines, which have relatively low energy throughputs, are not addressed by the 2002 circular or the 9/11 Commission Act; nevertheless, PSD officials have told us the security of these pipelines is important and should be addressed.

observed, one operator asked that the recommendations be put in writing, and PSD officials agreed to do so.

Standards for Internal Control in the Federal Government calls for deficiencies found during evaluations to be communicated to the individual responsible for the function and to at least one level of management above that individual. It also calls for information to be recorded and communicated to management and others within the entity who need it and in a form and within a time frame that enables them to carry out their internal control and other responsibilities. PSD officials explained they had reasons for not transmitting written recommendations to operators when they first started the CSR program, and they subsequently continued the practice of sharing recommendations orally.[53] However, by transmitting written recommendations to pipeline operators, PSD could better ensure that operators have clear guidance on actions they can take to enhance security.

PSD officials agreed that their pipeline security efforts would benefit from transmitting CSR recommendations to pipeline operators in writing and told us they intend to begin doing this after they issue new Pipeline Security Guidance and revise their CSR protocol.[54] However, they could not provide a specific time for when they would begin transmitting the recommendations to operators. Standard practices for project management call for developing a plan that includes defined approaches as well as start dates for activities.[55] Developing such a plan could help PSD accomplish its intended goal of transmitting CSR recommendations in writing to pipeline operators.

In addition, PSD officials told us they do not have a database of the recommendations they make to operators as a result of its CSRs; rather, they document CSR recommendations in individual internal reports PSD maintains on each operator. Having such a database could allow PSD to

[53] In trying to recall the origin of the decision to not communicate recommendations in writing, PSD officials said it was based on concerns about an operator's potential liability if it did not implement the recommendations and its pipeline system was later attacked. However, officials acknowledged that they send operators written recommendations for their newer program—the CFI program—without such concerns.

[54] PSD has contracted with Johns Hopkins University Applied Physics Laboratory to revise the CSR protocol.

[55] Project Management Institute, *A Guide to the Project Management Body of Knowledge* © (Fourth Edition, 2008).

analyze the recommendations it has made through the CSR program. Moreover, the officials said they do not have a process for following up on those recommendations other than through subsequent CSRs that, on average, occur about every 5 years. According to PSD's General Manager, the greatest challenge PSD officials face is that they do not know if operators are implementing the recommendations PSD makes as a result of the CSRs. He further stated that he would like to conduct CSRs with each pipeline operator about once every 2 or 2.5 years to see if operators have implemented PSD's recommendations, but with a small staff, PSD can only visit a company about once every 4 or 5 years.[56]

Similarly, PSD officials said they do not have a database that would allow them to readily analyze the CFI recommendations they make. The CFI program, designed as a one-time inspection program of every critical pipeline facility of the 100 most critical pipeline facilities, includes recommendations that PSD sends to pipeline operators and are specific to each facility it inspects. Although the CFI contractor designed a database to capture the results of each completed CFI, the database does not include the recommendations made. Furthermore, PSD officials said they to not have a process for following up to see if operators have implemented these recommendations.

Standards for Internal Control in the Federal Government state that internal controls should generally be designed to assure that ongoing monitoring occurs, and further states that monitoring should include policies and procedures for ensuring that the findings of reviews are promptly resolved. Because PSD does not follow up on its CSR recommendations other than through a subsequent CSR 5 years later, on average, it lacks assurance that its recommendations are being implemented and whether the state of pipeline security is improving. PSD officials agreed that having a database that would allow them to analyze CSR recommendations, and following up on recommendations more frequently and systematically could increase PSD's knowledge of the security posture and vulnerabilities of individual operators as well as the pipeline industry, enhance its ability to monitor security progress, and provide additional information about its pipeline security efforts. In carrying out its CFI program, PSD has invested resources in hiring a contractor, conducting inspections, making recommendations, and

[56] During the course of our review, the number of PSD staff ranged from 11 to 12. Three of these staff generally conducted CSRs.

developing a database. However, PSD officials agreed that without including its CFI recommendations in that database and following up on their implementation, they cannot analyze the recommendations they have made and have limited information on whether pipeline operators are addressing security vulnerabilities identified at each critical facility. PSD officials told us in May 2010 that they would like to follow up on the recommendations they make as a result of their inspections and had been discussing ways they do this, but they did not have specific plans or time frames for doing so.

Moreover, the 9/11 Commission Act states that DHS or DOT should issue pipeline security regulations if DHS determines they are appropriate. PSD officials told us in April 2009 that the results of the CSR and CFI programs, together, will inform that decision and noted that they are continually reassessing whether regulations are needed. They explained that they have been learning about the security posture of pipeline operators through these two programs and see indications that operators are making progress in improving security. Still, in a December 2009 quarterly report to the Office of Transportation Sector Network Management (TSNM) based on the first 159 CFIs, PSD reported that CFI data indicated that security improvements are needed. PSD further reported that regulations were not needed at that time. PSD officials agreed that by following up more frequently on whether operators are implementing the recommendations PSD makes as a result of its CSRs and developing a process for following up on the recommendations it makes as a result of its CFIs, they could be better informed of the state of the nation's pipeline security, including whether their recommendations have been implemented. Additionally, this would provide them information they say they plan to use to decide whether pipeline security regulations are needed.

PSD Has Developed Pipeline Security Recommendations

PSD reported that it met the 9/11 Commission Act mandate to develop and transmit security recommendations to pipeline operators through its issuance of Pipeline Security Smart Practices (Smart Practices). PSD issued its Smart Practices in August 2006 to reflect lessons learned from its first few years of conducting CSRs and to detail security practices that can enhance the security of the pipeline industry. The Smart Practices address a wide range of security practices, such as risk assessments, vulnerability assessments, and security planning; threat information; employment screening; vehicle checkpoints; physical security; intrusion detection; security awareness training; and drills, exercises, and regional cooperation. During CSRs, PSD officials remind operators of the Smart

Practices and disseminate the document. In addition, PSD officials told us they inform operators of its availability through activities such as at the annual International Pipeline Security Forum and disseminate it upon request. PSD intends to periodically review and update the Smart Practices to reflect advancements in security technology and maintain the viability of the security practices described.

In addition, PSD officials stated that they will further address this mandate by issuing new Pipeline Security Guidelines to replace the 2002 circular. According to these officials, the biggest difference between the existing and new draft pipeline security guidelines is that the new voluntary guidelines will apply to all pipeline operators—including those who do not have any critical facilities. Under the new guidelines, all operators will be expected to implement some security measures at all their facilities, and implement even more at critical facilities. In contrast, the 2002 circular applies only to those operators that have critical facilities. In addition, the new guidelines will contain a section on cyber security.[57] As of May 2010, PSD officials said that the new guidelines were in draft and expected they would be issued later in 2010.

PSD officials told us they worked closely with industry groups to develop the new draft guidelines, and industry groups we spoke with commended PSD's collaborative approach during this process. An INGAA official explained that PSD used an iterative process to develop the new guidelines that included holding multiple sessions with stakeholders and forming work groups. An APGA official spoke of the open process PSD used in inviting industry comments. Similarly, AGA officials spoke highly of PSD's approach of inviting operator and association participation, which they said contributed to new guidance that applies to critical infrastructure and provides sensible baseline guidance for operators—both large and small—for securing noncritical infrastructure. API and AOPL officials also said that PSD worked closely with them and commended PSD's coordination efforts.

[57] Some pipelines may be vulnerable to "cyber attacks" on computer control systems that are used to collect data from pipeline sensors in real time and display these data to controllers, who monitor the data and operate pipeline control equipment remotely. A pipeline operator's control system represents a significant investment on the part of the operator and is a critical resource for response and recovery in the event of a pipeline incident of almost any type.

PSD Officials Report Developing a Pipeline Security and Incident Recovery Protocols Plan

PSD officials stated that they have drafted a pipeline security and incident recovery protocols plan, which the 9/11 Commission Act required be completed by August 2009. The 9/11 Commission Act requires that DHS develop a pipeline security and incident recovery protocols plan that includes (1) increased federal security support to the most critical pipelines under severe security threat alert levels or specific threat information and (2) a plan to develop protocols for the continued transportation of natural gas and hazardous liquids to essential markets and for essential public health or national defense uses in the event of an incident. The act required DHS to submit a report to Congress by August 2009 that included the plan and the implementation costs of any recommendations in the plan.

The plan is also to take into account actions and plans of private and public entities and consult with DOT and other stakeholders specified in the 9/11 Commission Act. The act requires DHS to develop this plan in consultation with DOT and PHMSA and in accordance with the annex to the DOT/DHS MOU, the National Strategy for Transportation Security, and HSPD-7. The 9/11 Commission Act also identifies other parties that are to be consulted as DHS develops the plan.[58] According to PSD, it consulted with the various parties called for by the act in developing its plan. Starting in December 2008, PSD, in coordination with the DOT, conducted a series of meetings and interviews with DOE, DHS's Office of Infrastructure Protection, and the Federal Bureau of Investigation (FBI).[59] PSD subsequently held two workshops (in April and May 2009) at the Johns Hopkins University Applied Physics Laboratory to discuss and review the document with additional security partners and stakeholders. PSD informed us that in developing the plan, it consulted the

[58] The 9/11 Commission Act states that interstate and intrastate transmission and distribution pipeline operators, nonprofit employee organizations representing pipeline employees, emergency responders, offerors, state pipeline safety agencies, public safety officials, and any other relevant parties are to be consulted. The incident recovery protocols plan is also to be developed in conjunction with interstate and intrastate pipeline operators and terminal and facility operators connected to pipelines.

[59] The Office of Infrastructure Protection leads the coordinated national program to reduce risks to the nation's critical infrastructure and key resources posed by acts of terrorism, and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency.

representatives of numerous federal agencies and agency components, as well as nonfederal organizations and industry groups.[60]

As of March 2010, PSD officials said they had not submitted the required report to Congress. According to the officials, the pipeline security and incident recovery protocols plan had been reviewed within DHS and was being reviewed by the Office of Management and Budget. They further said the draft plan clarifies the roles of federal agencies during and after various types of incidents, but does not contain any new responsibilities or recommendations for federal agencies or industry. As such, there are no additional costs associated with the plan and the report to Congress will not include a cost estimate.

PSD Could Strengthen Its Documented Security Strategy and More Reliably Report Security Improvements

PSD's Security Strategy Could Be Strengthened by Incorporating Performance Measures and Milestones

The 2007 Pipeline Modal Annex to the Transportation Systems Sector-Specific Plan—TSA's national security strategy for pipeline systems—identified several goals and objectives for improving transportation and pipeline security; however, the strategy lacks performance measures and milestones. In prior work, we have identified the inclusion of performance measures and milestones as a desirable characteristic for a successful

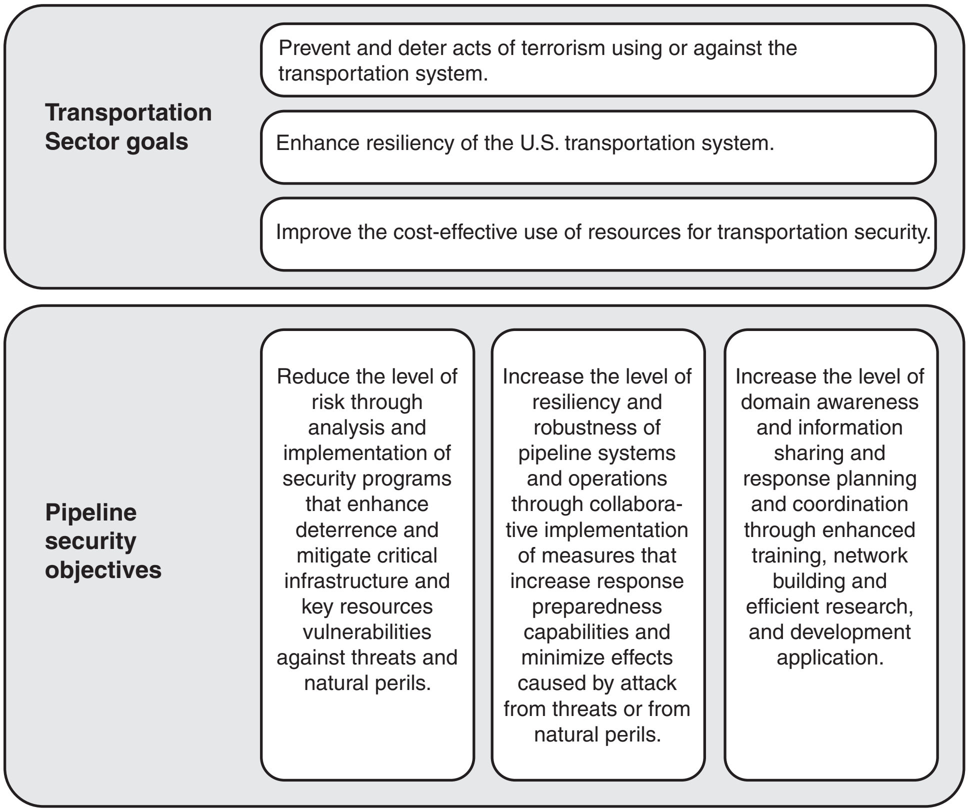
[60] PSD officials reported to us that they had coordinated the plan with DHS/TSA components and other DHS components, DOT/PHMSA, DOE, Department of Justice/FBI, Department of Interior/Minerals Management Service, National Transportation Safety Board, Federal Energy Regulatory Commission, Environmental Protection Agency, Federal Energy Regulatory Commission, Department of Defense/U.S. Army Corps of Engineers, National Association of Regulatory Utility Commissioners, National Association of State Energy Officials, National Governors Association, National Emergency Managers Association, National Association of Pipeline Safety Representatives, International Association of Fire Chiefs, International Association of Chiefs of Police, National Sheriff's Association, Pipeliners Union Local 798, Interstate Natural Gas Association of America, and Association of Oil Pipe Lines Owners/Operators.

national strategy and reported that a successful strategy should document what it seeks to achieve, the steps necessary to get those results, and the performance measures and milestones to gauge results.[61] We also reported that a strategy could accomplish this by stating its mission and then clearly linking its goals, objectives, programs, and performance measures to achieve results. PSD's strategy (the Pipeline Modal Annex) includes TSA's transportation sector goals that apply to all modes of transportation and identifies objectives specific to pipeline security, as shown in figure 10.[62] It also describes government and industry programs and activities that support these goals and objectives.

[61] In prior work we identified a set of desirable characteristics to aid responsible parties in further developing and implementing national strategies, and to enhance the usefulness of those strategies in resource and policy decisions and better ensure accountability. For a more detailed discussion of these characteristics, see GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

[62] The Pipeline Modal Annex also identifies supporting strategies PSD will pursue to achieve pipeline security objectives and presents information to explain what TSA, other federal components, or industry is doing and how those activities correspond with these strategies. For example, the Pipeline Modal Annex describes the CSR program as a program to promote the implementation of layered threat deterrence and vulnerability mitigation programs and to conduct network enhancement and information-sharing activities.

Figure 10: Transportation Sector Goals and Pipeline Security Objectives



Transportation Sector goals

- Prevent and deter acts of terrorism using or against the transportation system.
- Enhance resiliency of the U.S. transportation system.
- Improve the cost-effective use of resources for transportation security.

Pipeline security objectives

- Reduce the level of risk through analysis and implementation of security programs that enhance deterrence and mitigate critical infrastructure and key resources vulnerabilities against threats and natural perils.
- Increase the level of resiliency and robustness of pipeline systems and operations through collaborative implementation of measures that increase response preparedness capabilities and minimize effects caused by attack from threats or from natural perils.
- Increase the level of domain awareness and information sharing and response planning and coordination through enhanced training, network building and efficient research, and development application.

Source: GAO presentation of PSD information.

Although the Pipeline Modal Annex contains goals and objectives, it does not incorporate the performance measures and milestones PSD uses to evaluate the effectiveness of its security programs and activities.[63] For example, the annex describes an objective to reduce the level of risk through implementation of security programs and aligns it with the CSR program, but does not incorporate the performance measures and milestones PSD uses to evaluate the CSR program's effectiveness in achieving this objective. According to PSD officials, they considered performance measures and milestones in writing the annex, but did not

[63] According to PSD officials, they have prepared a 2010 revision to the 2007 Pipeline Modal Annex, which also does not incorporate performance measures and milestones. Officials told us in May 2010 that the revised annex was in internal review.

include them because the annex was intended as a planning document and not an assessment tool.

Our prior work concluded that better identification of performance measures and milestones would help parties achieve results in specific time frames and enable more effective oversight and accountability.[64] Thus, using milestones and performance measures to gauge progress in meeting its stated goals and objectives could help PSD further develop and implement its national security strategy for pipeline systems and enhance its usefulness in making resource and policy decisions to better ensure accountability. Moreover, by drawing a link in the pipeline security strategy between pipeline security goals and objectives, milestones, performance measures, and programs, PSD could better evaluate its progress in helping to improve pipeline security—information that could be useful to decision makers during the risk prioritization process—and achieve results in specific time frames.

PSD Has Taken Steps to Measure Its Performance, but Could Better Measure and More Reliably Report Industry Improvements

PSD has initiated efforts to measure its performance in helping strengthen the security of pipeline systems, but could improve its performance measures to better evaluate and reliably report on the extent of security improvements in the pipeline industry. As a part of its risk management framework, the NIPP calls for agencies to measure progress in security improvements against transportation sector goals, using performance measures—(1) output data to track the progression of tasks associated with a program or activity and (2) outcome data to evaluate the extent to which a program achieves sector goals and objectives. The NIPP also states that agencies must develop performance measures that are specific and clear about what they are measuring, practical in that the needed data are available, and built on objectively measured data. NIPP Metrics Program guidance, intended to help agencies develop performance measures, called for focusing on output measures in 2008, but continuing progress toward outcome-based performance measures in 2009.

PSD Has Developed Several Performance Measures

Although the national security strategy for pipeline systems—the Pipeline Modal Annex—does not include performance measures, PSD has developed two output measures and one outcome measure to help evaluate its progress in meeting program objectives, consistent with the requirements of the NIPP. For its output measures, PSD tracks

[64] See GAO-04-408T.

- the number of CSRs it conducts, with a milestone, or interim goal, of 12 CSRs each year; and
- the number of CFI trips it completes, with a milestone of 15 trips each year.[65]

According to PSD officials, they track CSR and CFI program progress against these two performance milestones, and provide this information to TSNM to consider in developing the transportation sector annual report.[66]

In addition, PSD officials told us that they collect performance output data on other activities and have established the following annual milestones:

- ten stakeholder conference calls,
- an International Pipeline Security Forum,
- quarterly meetings with DOT (per PHMSA's and TSA's annex to the MOU between DHS and DOT), and
- two pipeline Intermodal Security Training Exercise Program exercises.[67]

In 2009, PSD developed an outcome measure—the vulnerability gap—that uses CSR program data to help evaluate the impact of its efforts to improve pipeline security. This outcome measure is intended to evaluate improvements in operators' security planning and preparedness based on

[65] Each CFI trip involves inspections of multiple critical facilities.

[66] According to PSD and TSNM officials, an appendix to the 2010 Sector Critical Infrastructure and Key Resources Protection Annual Report for the Transportation Systems Sector will discuss other performance measures related to two risk mitigation activities—(1) the percentage of the 100 most critical pipeline systems that have had a CSR or a repeat CSR and (2) the percentage of the 100 most critical systems that have conducted annual security exercises and drills (specifically, the percentage that has participated in Intermodal Security Training Exercise Program exercises). As of May 2010, this report was in internal review.

[67] TSA's Intermodal Security Training Exercise Program offers an intermodal transportation security exercise program for transportation sector network communities. The program is intended to enhance the preparedness of the nation's surface transportation sector network with evaluations of prevention, preparedness, and the ability to respond to terrorist-related incidents.

its CSR program evaluations. More specifically, it compares the results of first and second CSRs to quantify the extent to which operators have reduced security vulnerabilities identified through CSRs.

Additional Outcome Measures Could Assist PSD in Measuring Pipeline Security Improvements

Although PSD has taken steps to gauge the progress of its programs, its ability to measure improvements in pipeline security is limited. The NIPP states that using performance measures as part of risk management can enable agencies to assess security improvements, and it instructs agencies to track progress toward a strategic goal or objective by measuring results or outcomes. The NIPP further states that the key to NIPP performance management is aligning outcome performance measures to goals and objectives.

According to the Transportation Systems Sector-Specific Plan, outcome measures should be used to assess program goals and objectives; however, output measures may be used as proxies for outcome measures in the early stages of its programs. In addition, we have reported on the limitations of output-based measures in our prior work. Specifically, we have stated that using output measures to evaluate security program performance may not systematically target areas of higher risk and may not result in the most effective use of resources because these measures are not pointed toward outcomes, or what activities are accomplishing.[68]

PSD's outcome measure—the vulnerability gap—measures aspects of two of its pipeline security objectives; however, PSD has not developed outcome measures that enable it to fully assess improvements related to pipeline security as a whole. The vulnerability gap focuses on what PSD measures through its CSR program—primarily improvements in pipeline operators' security planning and preparedness—but provides limited information on improvements in other areas, such as physical security. According to the Pipeline Modal Annex, the CSR program evaluates aspects of two of the pipeline security objectives—(1) to reduce risk and (2) to increase information sharing and response planning and coordination. By extension, the vulnerability gap measures these as well. For example, the vulnerability gap takes into account operators' risk reduction activities such as how they assess threats and vulnerabilities. It

[68] GAO, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Infrastructure*, GAO-06-91 (Washington, D.C.: December 15, 2005.)

also measures increased information sharing, such as how operators manage threat information.

However, according to the Pipeline Modal Annex, the CSR program does not evaluate the third pipeline security objective—to increase the level of resiliency and robustness of pipeline systems—and, thus, the vulnerability gap does not measure this objective.[69] As a result, PSD is limited in its ability to measure or report on improvements in this latter area of pipeline security. Furthermore, according to PSD officials, collecting CSR information every 4 to 5 years limits their ability to measure the security improvements that operators are making. Nevertheless, they said the changes they have observed from operators' first to second CSRs provide them with a strong level of confidence that improvements have occurred.

PSD officials explained that they are in the early stages of performance measurement and have not yet developed additional outcome measures or established time frames for doing so. We recognize challenges PSD might face in developing outcome measures related to reducing risk. In our prior work we acknowledged that assessing the deterrent benefits of a program is inherently challenging because it is often difficult to isolate the impact of an individual program on behavior that may be affected by multiple other factors.[70] In the case of pipeline security, it may be difficult to isolate the impact of PSD's programs on operators' security actions. Nevertheless, outcome-based data could better inform decision makers of the extent to which programs and activities have been able to reduce risk and better enable them to determine funding priorities within and across agencies. Also, developing additional outcome measures that assess the impacts of its efforts to improve pipeline security and are directly aligned with transportation sector goals and pipeline security objectives could better enable PSD to evaluate security improvements in the pipeline industry.

PSD Could Improve the Reliability of Data It Uses to Measure Effectiveness

PSD designed the vulnerability gap outcome measure to help evaluate the impact of its efforts to improve pipeline security using CSR program data, but the baseline data PSD used to measure its efforts may not be reliable. When PSD officials began conducting CSRs in 2003, they developed a CSR

[69] The Pipeline Modal Annex identifies other programs and activities that seek to increase resiliency and robustness.

[70] GAO, *Aviation Security: A National Strategy and Other Actions Would Strengthen TSA's Efforts to Secure Commercial Airport Perimeters and Access Controls*, GAO-09-399 (Washington, D.C.: September 30, 2009).

protocol to collect information on pipeline systems' corporate security planning and preparedness. However, according to PSD officials, they began using a different protocol in August 2004 that TSA developed for all surface transportation modes to use during their respective CSRs to ensure consistency among modes. Many questions in the second protocol differed from those in the first, although the topic areas were similar.[71]

Although changes in the CSR protocol provide PSD with more information on some topics, differences between the two protocols limited PSD's ability to use CSR program data collected with the first protocol. PSD officials explained they, therefore, sought to develop comparable CSR data for all operators, regardless of which protocol PSD used during CSRs. To accomplish this, PSD officials instructed staff to reconstruct a new protocol (using the second CSR protocol) for each pipeline operator PSD reviewed from mid-April 2003 through mid-July 2004—the 15-month period during which the first protocol was used.[72] Staff were to do this using available information from the first completed protocol, any notes PSD officials took during the CSR, and security plans or other documents PSD gathered during the CSR. However, PSD officials said they did not provide written instructions to staff or verify that staff accurately reconstructed the data. Although the officials expressed confidence in their staff's work, we could not be assured that the CSR information staff reconstructed was accurate and reliable.

We analyzed the content, or substance, of the questions in both the first and second protocols and identified concerns about whether operator information could have been transferred reliably from the first to the second protocol after the fact. We found that 41 of the 73 newer CSR protocol questions were either consistent with the content of the first protocol or could have been consistently verified using the security plan operators provided during the original CSR. We therefore found it reasonable that PSD staff would have been able to accurately transfer the completed information from the first protocol to the second protocol for these 41 questions. However, we could not be reasonably assured that PSD staff accurately transferred information for the remaining 32 questions onto the second protocol because the content of these questions was

[71] PSD subsequently made minor revisions to the second CSR protocol that did not affect our analysis or the data PSD uses for its outcome measure.

[72] According to PSD officials, they completed 31 CSRs from mid-April 2003 through mid-July 2004.

inconsistent and, thus, PSD staff may not have been able to reliably reconstruct the data using the security plans operators provided during the original CSRs. For example, the second protocol contained the following questions directed to operators, but we found no similar questions on the first protocol:

- Do you have a 24/7 emergency response/operations center?
- Do you conduct different levels of background checks based on type of employment (e.g., executive, operational, police)?
- Do you periodically conduct exercises and drills?

For these questions, and 29 others like them, PSD staff may have been able to locate the information they needed in notes and documents to reconstruct the second protocol, but we had no assurance that this was possible or done in an accurate and reliable manner. We have previously reported that performance measures should reliably assess progress such that the same results would be achieved if applied repeatedly to the same situation.[73] Furthermore, errors in data accuracy could alter conclusions about the extent to which performance goals have been achieved, such as reporting performance at either a higher or lower level than is actually being attained.

We have also reported that decision makers must have assurance that the program data being used to measure performance are sufficiently accurate and reliable if the data are to inform decision-making.[74] Thus, the usefulness of agency performance information depends to a large degree on the reliability and accuracy of performance data. Because of the changes in the CSR protocol questions and concerns about the reliability of reconstructed operator responses transferred to a different form, the baseline data PSD used in comparing operators' first and second CSR scores and resulting reports may not be accurate. As such, PSD's outcome performance measure—the differences in vulnerability gaps as calculated

[73] GAO, *Tax Administration: IRS Needs to Further Refine Its Tax Filing Season Performance Measures*, GAO-03-143 (Washington, D.C.: Nov. 22, 2002). In this report, GAO reported on nine key attributes of successful performance measures including the reliability of measures.

[74] GAO, *Managing for Results: Challenges Agencies Face in Producing Credible Performance Information*, GAO-GGD-00-52 (Washington, D.C.: Feb. 4, 2000).

using CSR scores—suggests a level of precision that may not be supported.[75] PSD officials said they did not see this as a significant problem because not all the baseline CSRs involved reconstructed data and, as they continue to conduct CSRs, they will eventually be able to compare the results of operators' second to third CSRs in reporting improvements. Furthermore, although PSD's CSR data may be useful for some analytical purposes, such as analyzing industry trends and assessing individual operators' security planning and preparedness, some of the early data are not useful for reporting the extent to which the vulnerability gap has closed. PSD and decision makers could be better informed and could more effectively prioritize efforts if PSD maintains a more reliable baseline for its outcome performance measure and does not use reconstructed data in reporting its baseline.

Conclusions

Securing the nation's vast network of hazardous liquid and natural gas pipeline systems is a formidable task. The importance of pipeline systems to the nation's economy underscores the need for PSD to employ a risk management approach to prioritize its security efforts. PSD has taken actions to implement a risk management approach, including identifying the 100 pipeline systems it considers most critical and being the first of the surface transportation modes to develop a risk assessment model. Nevertheless, work remains to ensure that the highest risk pipeline systems are given the necessary scrutiny. PSD's risk assessment model is in its early stages of development; however, information is available or expected that could enhance the vulnerability and consequence components of the model. By developing a plan that includes time frames and milestones for adding information to its risk assessment model, PSD could be better assured of reaching its goal to improve the model. This could help PSD more accurately rank pipeline systems according to risk and help guide resource allocation decisions. In addition, documenting a methodology for scheduling CSRs and CFIs that includes a pipeline system's risk ranking as the primary criteria, while recognizing other considerations that can affect scheduling, could help PSD ensure it prioritizes its oversight of pipeline systems that are most at risk.

PSD has taken actions to encourage private pipeline operators to employ security measures that will protect their pipeline systems, including

[75] An operator's CSR score is calculated based on the 73 standard questions in the newer CSR protocol.

critical facilities. While PSD officials have said that operators of the most critical pipeline systems are generally implementing voluntary security measures, two of PSD's key efforts—its CSR and CFI programs—have identified shortcomings in operators' security programs and critical facilities that should be addressed to reduce vulnerabilities. As such, an important aspect of the CSR and CFI programs is the specific recommendations PSD makes and tailors to each operator to address the vulnerabilities PSD has identified. However, PSD is missing opportunities with respect to these recommendations. PSD officials agreed that routinely transmitting CSR recommendations in writing to operators could better ensure that operators are clear on the actions they can take to enhance the security of their pipeline system or systems, and they have said they intend to do this. Developing a plan that includes a defined approach and time frames for how and when PSD intends to begin transmitting CSR recommendations in writing to pipeline operators could help PSD accomplish its intended goal.

In addition, by establishing databases of the CSR and CFI recommendations it makes, PSD could more readily and systematically analyze its recommendations and be better informed of security vulnerabilities in the pipeline industry. Furthermore, because CSRs take place infrequently and CFIs are not repeated, following up on the implementation of CSR and CFI recommendations is particularly important. By doing so, PSD could enhance its knowledge of the state of security of the pipeline industry as well as individual systems and facilities, have an additional means for measuring the effectiveness of its programs, and obtain information that could help inform its decision on whether it would be appropriate to issue pipeline security regulations.

The 2007 Pipeline Modal Annex represents a positive step toward conveying TSA's strategy for helping the pipeline industry secure the nation's pipelines. However, incorporating PSD's performance measures and milestones and linking them to the goals and objectives in its national security strategy for pipeline systems could aid PSD and the pipeline industry in achieving results within specific time frames and could facilitate more effective oversight and accountability. PSD has developed some output-based performance measures and milestones to track the progress of its programs and activities and has developed an outcome measure to evaluate the impact of some of its efforts to improve pipeline security. However, PSD's dependence on a single outcome measure hinders its ability to evaluate the extent of improvements related to all of its pipeline security objectives. Developing additional outcome measures aligned with its objectives could facilitate PSD's efforts to better evaluate its performance.

Moreover, PSD has collected data on the security posture of pipeline operators through its CSR program and compared vulnerability gap data over time to measure the progress operators have made. PSD's CSR data may be useful to PSD for various analytical purposes. However, because of reliability issues affecting the baseline data PSD uses for calculating its vulnerability gap outcome measure, PSD would be better informed if, going forward, it establishes reliable baseline data for measuring and reporting improvements in pipeline security. Although this would limit PSD's ability to report on improvements in operators' security efforts from the first 15 months of the CSR program, it could provide greater assurance that, in the future, PSD is more accurately and reliably measuring those pipeline security improvements.

Recommendations for Executive Action

To improve aspects of the Pipeline Security Division's (PSD) efforts to help ensure pipeline security, we recommend that the Assistant Secretary for the Transportation Security Administration take the following eight actions.

To ensure that PSD is managing risk effectively,

- Develop a plan with time frames and milestones for improving the data in the pipeline risk assessment model by, for example, adding more data to the consequence component.
- Document a methodology for scheduling Corporate Security Reviews (CSR) and Critical Facility Inspections (CFI) that considers a pipeline system's risk ranking as the primary scheduling criteria and balances it with other practical considerations.

To help PSD maximize its CSR and CFI efforts and keep its knowledge of the security posture of the pipeline industry current,

- Develop a plan that includes a defined approach and time frame for how and when PSD intends to begin transmitting CSR recommendations in writing to pipeline operators.
- Establish a database of CSR recommendations and develop a process for following up on the implementation of those recommendations.

- Establish a database of CFI recommendations and develop a process for following up on the implementation of those recommendations.

To better achieve the security strategy laid out in the Pipeline Modal Annex—the national security strategy for pipeline systems—to the extent feasible, revise future updates of the annex to incorporate performance measures for assessing PSD and pipeline industry progress and link those measures to pipeline security objectives.

To better evaluate PSD's performance in helping strengthen the security of hazardous liquid and natural gas pipelines and improvements in pipeline security, develop additional outcome measures that are directly linked to sector goals and modal objectives and track progress towards its stated pipeline security objectives.

To help ensure reliable reporting of security improvements in the pipeline industry, establish reliable baseline data and, until that time, refrain from using reconstructed baseline data to report progress in closing the vulnerability gap.

Agency Comments and Our Evaluation

We provided a draft of our report to DHS on July 2, 2010, for review and comment. On July 23, 2010, DHS provided written comments, which are reprinted in appendix II. In commenting on the draft report, DHS stated that it concurred with our findings and all eight recommendations and discussed efforts planned or underway to address them. However, the actions DHS reports it plans to take do not fully address the intent of four of our eight recommendations.

DHS concurred with our first recommendation that TSA develop a plan with time frames and milestones for improving the data in the pipeline risk assessment model and stated that PSD will develop a plan to coordinate security efforts that are underway that will help refine the pipeline risk ranking tool (the pipeline risk assessment model). DHS further stated that additional data from critical facility inspections, the hazardous liquid pipeline assessment, and toxic inhalation hazard study, among others, will help inform the consequence component. We support PSD's intention to develop a plan for taking such action and further encourage TSA to consider using critical facility inspection data to inform the vulnerability component of the pipeline risk model. The development of a plan for improving the data in the pipeline risk assessment model will address the intent of our recommendation, provided it includes time frames and milestones.

DHS concurred with our second recommendation that TSA document a methodology for scheduling CSRs and CFIs that considers a pipeline system's risk ranking as the primary scheduling criteria and balances it with other practical considerations. DHS stated that TSA's analysis identified as critical those pipeline systems that transport the greatest amount of energy and that PSD developed the risk ranking tool to further enhance its risk-based effort. DHS further stated that to increase the value of the risk ranking tool, PSD will develop additional data to inform the tool's rankings and base its programmatic efforts on the results. While we support PSD's intention to develop additional data to inform its ranking of pipeline systems based on risk and base programmatic efforts on those rankings, these actions, alone, will not fully address the intent of our recommendation. We believe that to better prioritize oversight of pipeline systems among the 100 that are the most critical, and to address our recommendation, TSA should document a methodology for how it will schedule pipeline CSRs and CFIs in a manner that considers risk as the primary scheduling criteria, while balancing other practical scheduling considerations, such as travel efficiencies.

DHS concurred with our third recommendation that TSA develop a plan that includes a defined approach and time frame for how and when PSD intends to begin transmitting written CSR recommendations to pipeline operators. DHS stated that PSD intends to modify its process of providing oral recommendations for security improvements to pipeline operators to include providing these recommendations to operators in writing. Developing a plan that includes a defined approach for how it will transmit its written recommendations to operators and a time frame for when it will begin to do so will address the intent of our recommendation.

DHS concurred with our fourth recommendation that TSA establish a database of pipeline CSR recommendations and develop a process for following up on the implementation of those recommendations. DHS stated that PSD will initiate the development of such a database and further stated that repeat CSRs will particularly focus on the implementation of recommendations from prior reviews. Developing a database will partially address this recommendation. However, while we support a plan that includes PSD following up on prior CSR recommendations during subsequent CSRs, this, alone, will not fully address the intent of our recommendation. Because PSD conducts a CSR for any given pipeline operator about every 5 years, on average, a process for additional and timelier follow up is needed if PSD is to be assured that its recommendations are being implemented.

DHS concurred with our fifth recommendation that PSD establish a database of CFI recommendations and develop a process for following up on the implementation of those recommendations. DHS stated that PSD has initiated the development of a CFI recommendation database and further stated that following up on those recommendations will enable TSA to assess the pipeline industry's progress in mitigating identified security deficiencies. Completing this database and developing a process for following up on the CFI recommendations will address the intent of our recommendation.

DHS concurred with our sixth recommendation that TSA revise future updates of the Pipeline Modal Annex to incorporate performance measures for assessing PSD and pipeline industry progress and link those measures to pipeline security objectives. DHS stated that in future updates to the Transportation Systems Sector-Specific Plan, PSD will include performance measures within the Pipeline Modal Annex consistent with the sector format and guidance. However, direction on what is to be included in future updates of the Pipeline Modal Annex originates with TSA, which provides transportation modes, including pipeline, with guidance and a recommended format on how to revise or rewrite modal annexes to the Transportation Systems Sector-Specific Plan. TSA's 2010 Modal Plan Revision Guidance for transportation modes does not explicitly call for incorporating performance measures for assessing modal progress and, further, linking those measures to modal objectives. Thus, without TSA direction to include performance measures that are linked to objectives in modal annex updates, the action DHS described to address our recommendation does not fully address our intent.

DHS concurred with our seventh recommendation that TSA develop additional outcome measures that are directly linked to sector goals and modal objectives and track progress towards its stated pipeline security objectives. DHS stated that PSD will develop appropriate outcome measures that reflect the impact of its security programs and the security status of the pipeline industry, and further stated that this effort will be made consistent with the performance measurement guidance of the Transportation Systems Sector-Specific Plan. We support PSD's intention to develop additional outcome measures. However, to fully address the intent of our recommendation, TSA should ensure that its performance measurement guidance calls for outcome measures to be directly linked to sector goals and modal objectives.

DHS concurred with our eighth recommendation that TSA establish reliable baseline data for reporting security improvements in the pipeline industry and, until that time, refrain from using reconstructed baseline data to report progress in closing the vulnerability gap. DHS stated that updated data from repeat CSRs will be utilized to ensure more accurate reporting of the pipeline industry's security status. Such action will address the intent of our recommendation.

DHS also provided us with technical comments, which we considered and incorporated in the report where appropriate.

As agreed with your office, unless you publicly announce the contents of the report, we plan no further distribution for 30 days from the report date. At that time, we will send copies to the Secretary of Homeland Security, the Assistant Secretary of the Transportation Security Administration, appropriate congressional committees, and other interested parties. The report also is available at no charge on the GAO Web site at http://www.gao.gov/.

If you or your staff have any further questions about this report or wish to discuss these matters further, please contact me at (202) 512-4379 or lords@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 III.

Stephen Lord

Stephen M. Lord
Director, Homeland Security and Justice Issues

Appendix I: Objectives, Scope, and Methodology

Objectives

You requested that we review the Transportation Security Administration's (TSA) efforts to help ensure pipeline security. Specifically, this report addresses the following questions:

- To what extent has TSA's Pipeline Security Division (PSD) identified critical pipeline systems, assessed risk, and prioritized efforts, consistent with the National Infrastructure Protection Plan (NIPP), to help strengthen the security of hazardous liquid and natural gas pipeline systems?
- To what extent has PSD taken actions to implement agency guidance and requirements of the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act) regarding the security of hazardous liquid and natural gas pipeline systems?
- To what extent has PSD measured its performance to help strengthen the security of hazardous liquid and natural gas pipeline systems and improvements in pipeline security?

Scope and Methodology

To determine the extent to which PSD used a risk management process to help strengthen the security of pipelines, we reviewed PSD's efforts to (1) identify critical pipeline systems, (2) assess risk, and (3) prioritize its pipeline review and inspection efforts. To evaluate PSD's efforts to identify the most critical pipeline systems, we reviewed relevant documents, including PSD's list of the 100 most critical pipeline systems, and interviewed PSD officials about the methods they used to identify the most critical pipeline systems.

To evaluate PSD's efforts to assess risk, we reviewed TSA assessments of threat, vulnerability, and consequence that were conducted from 2003 through May 2010. Specifically, we reviewed TSA's Pipeline Threat Assessments for 2008 and 2010 and interviewed officials at TSA's Office of Intelligence. We also reviewed Corporate Security Reviews (CSR) that PSD uses as vulnerability assessments, and consequence assessments on natural gas disruptions sponsored by the Department of Energy and PSD—and discussed these assessments with relevant agency officials. TSA characterized these as threat, vulnerability, and consequence assessments, but we did not assess the extent to which these assessment activities met the NIPP criteria for threat, vulnerability, and consequence assessments, as this analysis was outside the scope of our work.

To evaluate PSD's efforts to prioritize risk, we analyzed its risk assessment model—the Pipeline Relative Risk Ranking Tool, which integrates the various assessments to produce a risk estimate and relative risk ranking for each pipeline system—and the data PSD inputs into the model. We also interviewed PSD officials about how they decide when to schedule CSRs and Critical Facility Inspections (CFI). Using correlation analysis and the data in the pipeline risk assessment model, we compared the time elapsed between PSD's first and subsequent CSR for each pipeline system with the system's ranking based on risk to measure the strength of their relationship.[1] Specifically, for those systems that had two CSRs, we assessed the strength of the correlation between the time elapsed from the first and second CSR and the system's risk ranking. We found a correlation coefficient of 0.2, which indicates a weak correlation. A correlation coefficient measures the strength and direction of linear association between two variables without controlling for the effects of other characteristics.

Because PSD officials said that the time elapsed between CSRs might be misleading because it does not account for other significant contact PSD might have had with an operator during that period, such as through a CFI, we controlled for this by running a simple regression equation.[2] Specifically, the regression equation compared the time elapsed between the first and second CSR against system risk rank and a dummy variable to denote if PSD inspected at least one critical facility belonging to an operator between the first and second CSR. This regression equation explained about 21 percent of the total variation in elapsed time between the first and second CSR. To determine the extent to which PSD prioritized the CFIs it conducted, we performed a correlation analysis to measure the strength and direction of the relationship between a system's risk ranking and the order in which PSD conducted a first CFI for that system compared with other systems. We found a correlation coefficient of 0.03, which denotes that almost no correlation exists between the two variables.

To assess the reliability of the April 2003 through May 2010 data PSD used in its risk assessment model, we (1) performed electronic testing of

[1] For pipeline operators that operate more than one system, we used only the highest risk-ranked system for that operator in our analysis to control for the possibility that PSD also conducted a second CSR for a lower risk system belonging to the same operator.

[2] Although PSD officials might have contact with pipeline operators through means other than CSRs and CFIs, we could not quantify other forms of contact and, therefore, could not include them in the analysis.

required data elements, (2) compared data in the model with other sources of information, and (3) interviewed agency officials knowledgeable about the data. We determined that the data were sufficiently reliable for the purposes of this report. We analyzed agency guidance on risk management, including the NIPP and the Transportation Systems Sector-Specific Plan, to determine criteria for effectively implementing a risk management framework and associated best practices for conducting risk assessments, and compared these with PSD's risk management strategy. In addition, we compared PSD's approach for advancing its risk management program to standard practices in program management planning.[3]

To determine the extent to which PSD has taken actions to implement agency guidance and 9/11 Commission Act requirements regarding pipeline security, we reviewed the Pipeline Security Information Circular (2002 circular) and the 9/11 Commission Act and actions described in agency documents. These documents included PSD's Pipeline Modal Annex, CSR Standard Operating Procedures, CSR and CFI protocols, and Pipeline Security Smart Practices.[4] To learn more about PSD's actions, we interviewed officials from PSD and DOT as well as representatives of the major associations with ties to the pipeline industry (American Petroleum Institute, Association of Oil Pipe Lines, American Gas Association, and Interstate Natural Gas Association of America, and American Public Gas Association); attended the 2008 International Pipeline Security Forum organized by PSD and Natural Resources Canada; and met with security personnel from 10 pipeline operators with headquarters or significant operations in Houston. We chose Houston because it has the highest concentration of operators with systems on PSD's list of the 100 most critical pipeline systems, and those with whom we met operate about one-third of those systems. While the results of these interviews cannot be generalized to all pipeline operators, they provided perspectives on how operators view PSD's security efforts.

To further our understanding of PSD's review and inspection processes, pipeline operators' security planning efforts, and physical security measures in place at selected critical pipeline facilities, we accompanied PSD officials on four reviews of pipeline systems operated by four different operators and 10 inspections of critical facilities operated by

[3] The Project Management Institute, *The Standard for Program Management* © (2006).

[4] Our review of the 2002 circular included the Pipeline Security Contingency Planning Guidance.

three different operators. We observed these reviews and inspections because PSD had scheduled them while we were conducting our work. These involved hazardous liquid and natural gas pipelines as well as different size operators with pipeline systems that varied in the amount of energy they carry, their relative risk ranking, and their location (we observed CSRs in four states and CFIs in three states). These observations further included one cross-border pipeline system and one port facility regulated under the Maritime Transportation Security Act. While the results of these observations cannot be generalized to all CSRs and CFIs or all pipeline systems and critical facilities, they provided us with an understanding of how PSD conducts these reviews and inspections, and some perspective on the security posture at different critical facilities. We also interviewed representatives of Secure Solutions International—a security and risk management consulting firm that assisted PSD in developing and carrying out CFIs—about critical facilities and the inspection process. In addition, we independently observed the exterior of 10 other critical facilities. We selected these facilities, which were located in four states and operated by six different operators, because of their proximity to GAO offices. Although the results of these observations cannot be generalized to all critical facilities, they provided us insight on security measures at additional critical facilities.

We also compared PSD's processes for transmitting and following up on CSR and CFI recommendations with criteria in the Standards for Internal Control in the Federal Government regarding the monitoring of deficiencies found during evaluations.[5] In addition, we compared PSD's approach for advancing its process for communicating CSR recommendation to standard practices in project management.[6]

To determine the extent to which PSD measured the impact of its efforts to help strengthen the security of pipelines and improvements in pipeline security, we reviewed PSD's performance measures and milestones. We analyzed TSA's national security strategy for pipeline systems—the 2007 Pipeline Modal Annex—to determine the extent to which it conformed to provisions related to goal setting and performance measurement found in

[5] GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).

[6] Project Management Institute, *A Guide to the Project Management Body of Knowledge* © (Fourth Edition, 2008).

Executive Order 13416: Strengthening Surface Transportation Security[7] and guidance on desirable characteristics for a national strategy that we developed in a previous report.[8] We also interviewed Office of Transportation Sector Network Management (TSNM) and PSD officials regarding PSD's performance measures and milestones and related data collection methodologies. In addition, we reviewed the 2009 NIPP and the 2007 Transportation Systems Sector-Specific Plan to determine the risk management framework's recommended approach to performance measurement and compared TSA's actions to that guidance.

To assess the reliability of the data PSD used to develop its vulnerability gap outcome measure in 2009 for reporting on the extent of improvements in pipeline security, we reviewed and analyzed related documentation and interviewed PSD officials knowledgeable about the data and PSD's data collection methods. As part of this analysis, we compared two successive data collection instruments—the original CSR protocol that PSD developed and used in conducting CSRs from April 2003 to July 2004 and a newer protocol that PSD officials said they began using in August 2004, after TSA developed a protocol to be used by all the transportation modes.

More specifically, to analyze and categorize specific differences between the two protocols, two analysts compared the first and second protocols to determine the extent to which content from the 73 questions in the newer protocol corresponded with content in the original protocol. To ensure the validity and reliability of our analysis, the two analysts discussed and reconciled any differences. With the assistance of a methodologist, the analysts mutually agreed on how to categorize their assessment of the newer protocol questions. They agreed on the following two categories to describe whether the information could have been reliably transferred from one protocol to the other:

- We were reasonably assured that PSD staff would have been able to accurately transfer completed information from the first protocol to the second.

[7] Exec. Order No. 13,416, 71 Fed. Reg. 71,033 (Dec. 5, 2006).

[8] GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

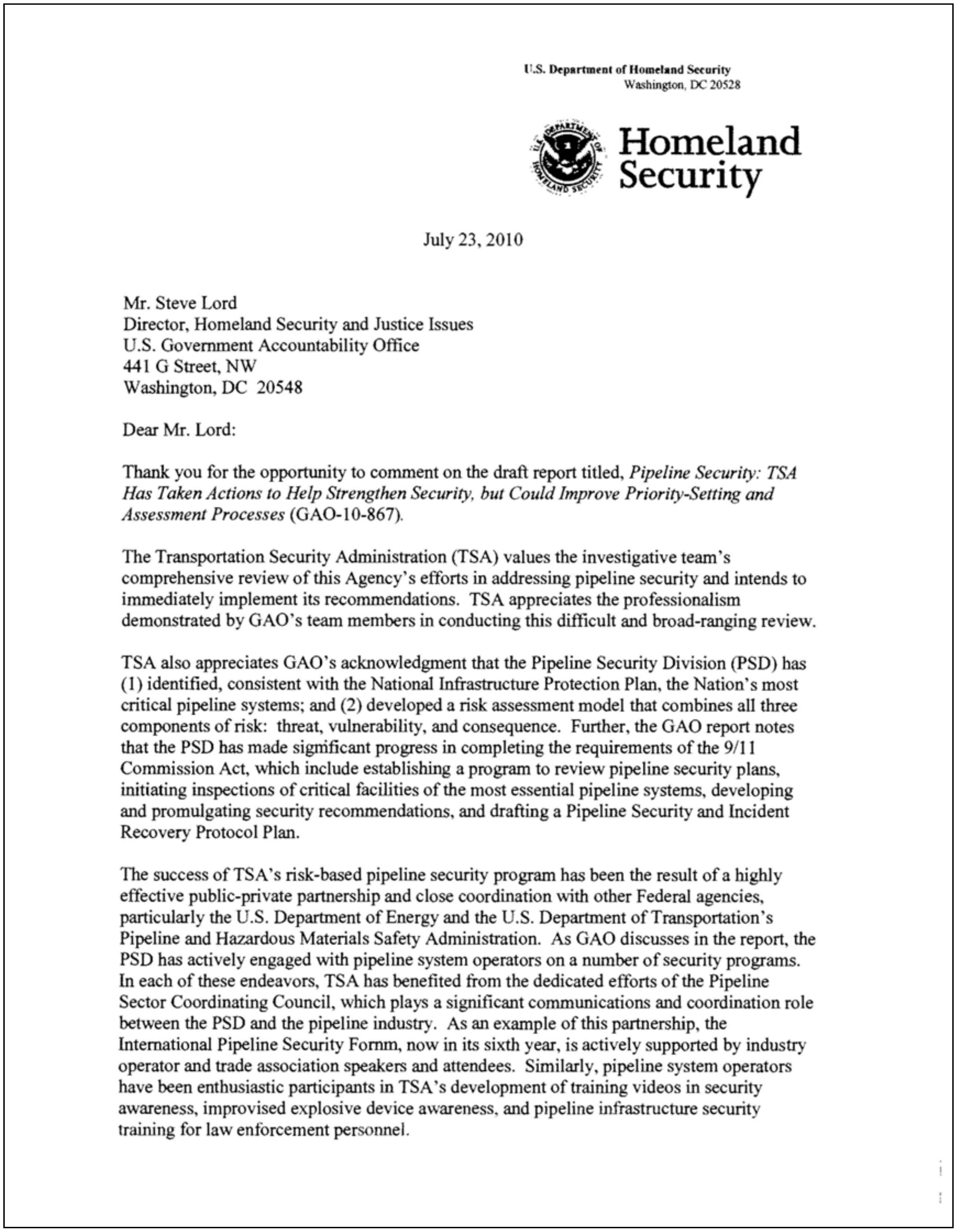
- We could not be reasonably assured that PSD staff would have been able to accurately transfer completed information from the first protocol to the second.

Because we could not be reasonably assured of the accuracy of the transferred data, we concluded that some of the baseline data key to PSD's outcome measure may not be reliable, as called for in our prior work that describes nine key attributes of successful performance measures.[9] Furthermore, we determined that these data were not sufficiently reliable for the purposes of this report.

We conducted this performance audit from November 2008 to August 2010 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.

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

Appendix II: Comments from the Department of Homeland Security



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

Homeland
Security

July 23, 2010

Mr. Steve Lord
Director, Homeland Security and Justice Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

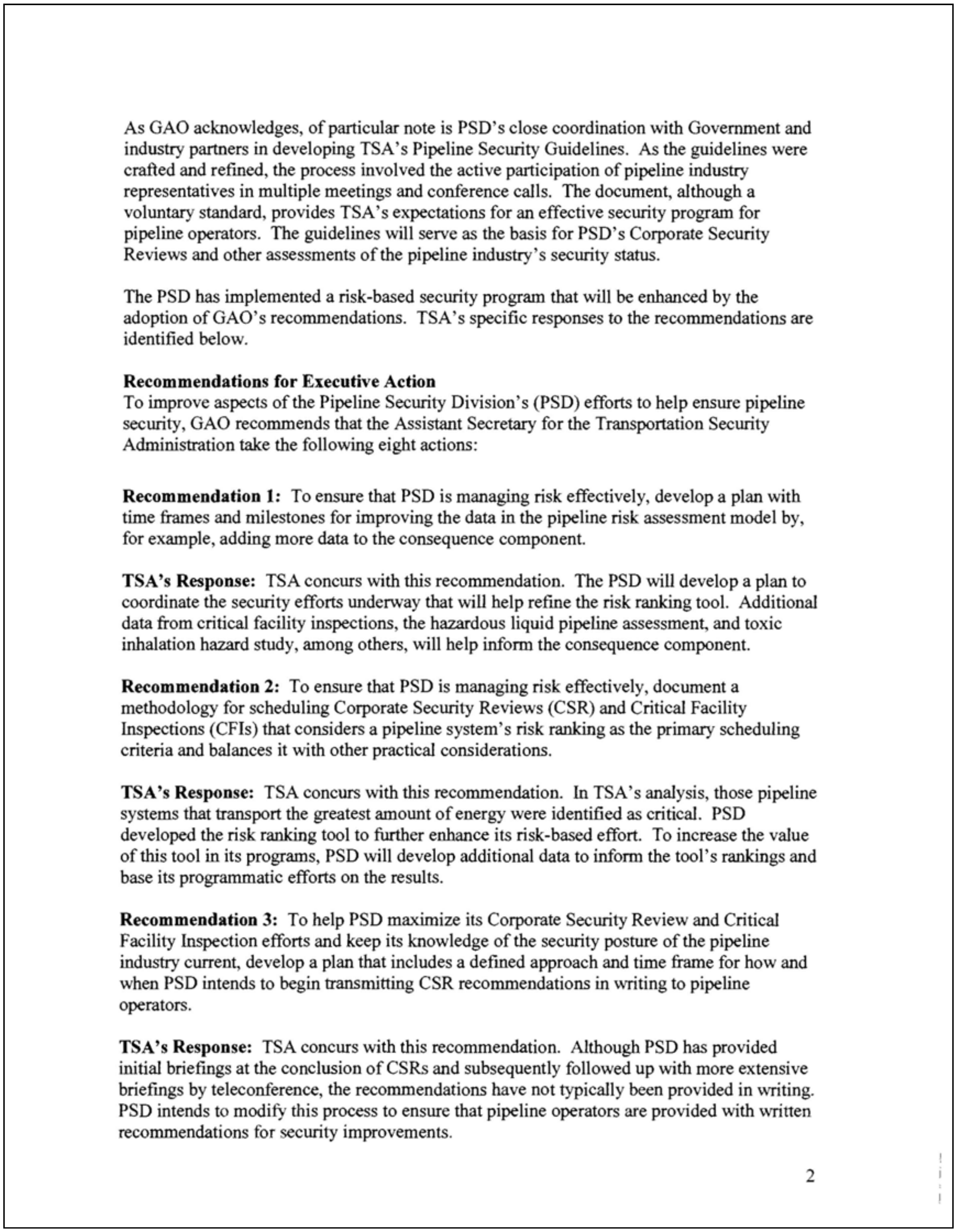
Dear Mr. Lord:

Thank you for the opportunity to comment on the draft report titled, *Pipeline Security: TSA Has Taken Actions to Help Strengthen Security, but Could Improve Priority-Setting and Assessment Processes* (GAO-10-867).

The Transportation Security Administration (TSA) values the investigative team's comprehensive review of this Agency's efforts in addressing pipeline security and intends to immediately implement its recommendations. TSA appreciates the professionalism demonstrated by GAO's team members in conducting this difficult and broad-ranging review.

TSA also appreciates GAO's acknowledgment that the Pipeline Security Division (PSD) has (1) identified, consistent with the National Infrastructure Protection Plan, the Nation's most critical pipeline systems; and (2) developed a risk assessment model that combines all three components of risk: threat, vulnerability, and consequence. Further, the GAO report notes that the PSD has made significant progress in completing the requirements of the 9/11 Commission Act, which include establishing a program to review pipeline security plans, initiating inspections of critical facilities of the most essential pipeline systems, developing and promulgating security recommendations, and drafting a Pipeline Security and Incident Recovery Protocol Plan.

The success of TSA's risk-based pipeline security program has been the result of a highly effective public-private partnership and close coordination with other Federal agencies, particularly the U.S. Department of Energy and the U.S. Department of Transportation's Pipeline and Hazardous Materials Safety Administration. As GAO discusses in the report, the PSD has actively engaged with pipeline system operators on a number of security programs. In each of these endeavors, TSA has benefited from the dedicated efforts of the Pipeline Sector Coordinating Council, which plays a significant communications and coordination role between the PSD and the pipeline industry. As an example of this partnership, the International Pipeline Security Fornm, now in its sixth year, is actively supported by industry operator and trade association speakers and attendees. Similarly, pipeline system operators have been enthusiastic participants in TSA's development of training videos in security awareness, improvised explosive device awareness, and pipeline infrastructure security training for law enforcement personnel.



As GAO acknowledges, of particular note is PSD's close coordination with Government and industry partners in developing TSA's Pipeline Security Guidelines. As the guidelines were crafted and refined, the process involved the active participation of pipeline industry representatives in multiple meetings and conference calls. The document, although a voluntary standard, provides TSA's expectations for an effective security program for pipeline operators. The guidelines will serve as the basis for PSD's Corporate Security Reviews and other assessments of the pipeline industry's security status.

The PSD has implemented a risk-based security program that will be enhanced by the adoption of GAO's recommendations. TSA's specific responses to the recommendations are identified below.

Recommendations for Executive Action
To improve aspects of the Pipeline Security Division's (PSD) efforts to help ensure pipeline security, GAO recommends that the Assistant Secretary for the Transportation Security Administration take the following eight actions:

Recommendation 1: To ensure that PSD is managing risk effectively, develop a plan with time frames and milestones for improving the data in the pipeline risk assessment model by, for example, adding more data to the consequence component.

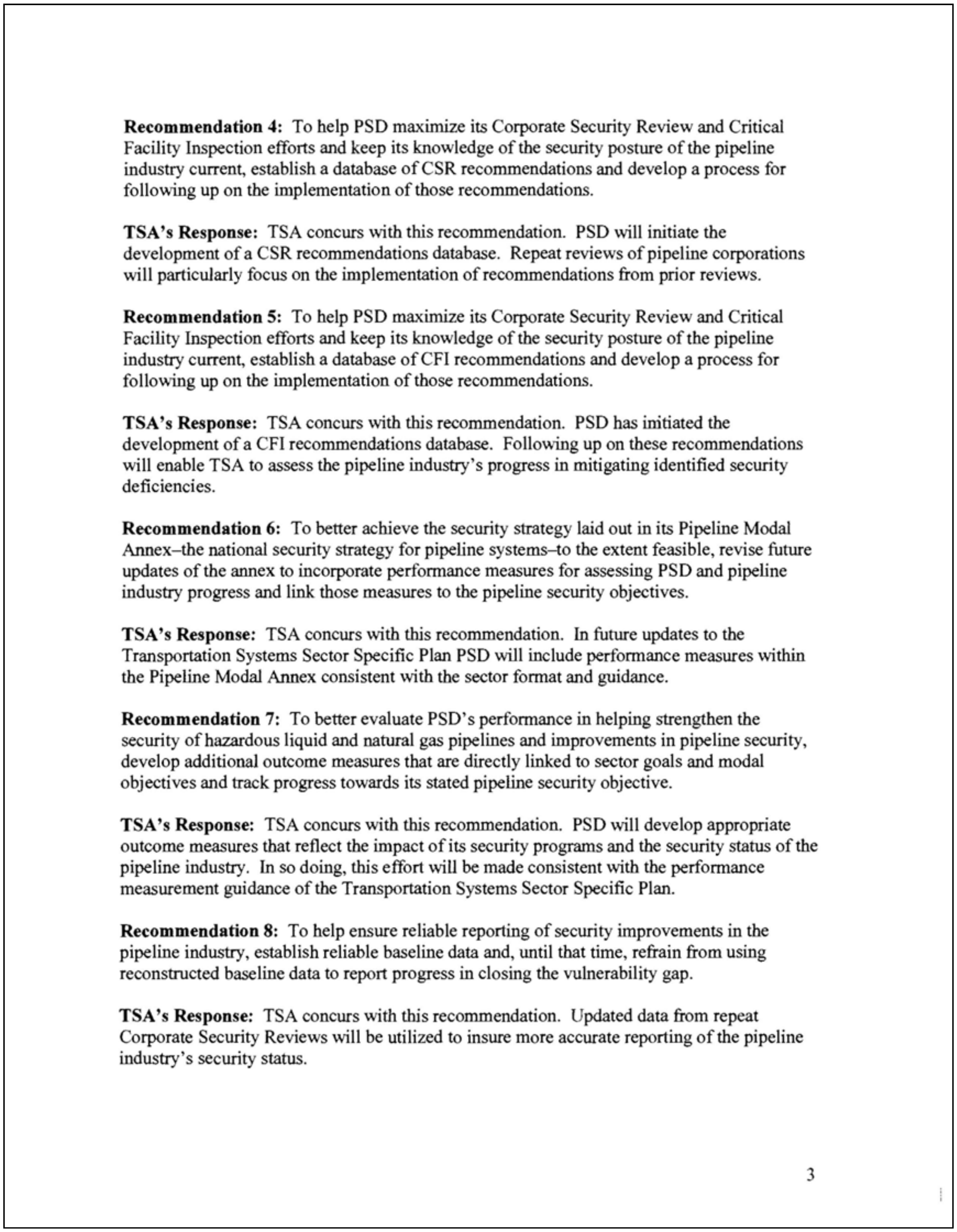
TSA's Response: TSA concurs with this recommendation. The PSD will develop a plan to coordinate the security efforts underway that will help refine the risk ranking tool. Additional data from critical facility inspections, the hazardous liquid pipeline assessment, and toxic inhalation hazard study, among others, will help inform the consequence component.

Recommendation 2: To ensure that PSD is managing risk effectively, document a methodology for scheduling Corporate Security Reviews (CSR) and Critical Facility Inspections (CFIs) that considers a pipeline system's risk ranking as the primary scheduling criteria and balances it with other practical considerations.

TSA's Response: TSA concurs with this recommendation. In TSA's analysis, those pipeline systems that transport the greatest amount of energy were identified as critical. PSD developed the risk ranking tool to further enhance its risk-based effort. To increase the value of this tool in its programs, PSD will develop additional data to inform the tool's rankings and base its programmatic efforts on the results.

Recommendation 3: To help PSD maximize its Corporate Security Review and Critical Facility Inspection efforts and keep its knowledge of the security posture of the pipeline industry current, develop a plan that includes a defined approach and time frame for how and when PSD intends to begin transmitting CSR recommendations in writing to pipeline operators.

TSA's Response: TSA concurs with this recommendation. Although PSD has provided initial briefings at the conclusion of CSRs and subsequently followed up with more extensive briefings by teleconference, the recommendations have not typically been provided in writing. PSD intends to modify this process to ensure that pipeline operators are provided with written recommendations for security improvements.



Recommendation 4: To help PSD maximize its Corporate Security Review and Critical Facility Inspection efforts and keep its knowledge of the security posture of the pipeline industry current, establish a database of CSR recommendations and develop a process for following up on the implementation of those recommendations.

TSA's Response: TSA concurs with this recommendation. PSD will initiate the development of a CSR recommendations database. Repeat reviews of pipeline corporations will particularly focus on the implementation of recommendations from prior reviews.

Recommendation 5: To help PSD maximize its Corporate Security Review and Critical Facility Inspection efforts and keep its knowledge of the security posture of the pipeline industry current, establish a database of CFI recommendations and develop a process for following up on the implementation of those recommendations.

TSA's Response: TSA concurs with this recommendation. PSD has initiated the development of a CFI recommendations database. Following up on these recommendations will enable TSA to assess the pipeline industry's progress in mitigating identified security deficiencies.

Recommendation 6: To better achieve the security strategy laid out in its Pipeline Modal Annex–the national security strategy for pipeline systems–to the extent feasible, revise future updates of the annex to incorporate performance measures for assessing PSD and pipeline industry progress and link those measures to the pipeline security objectives.

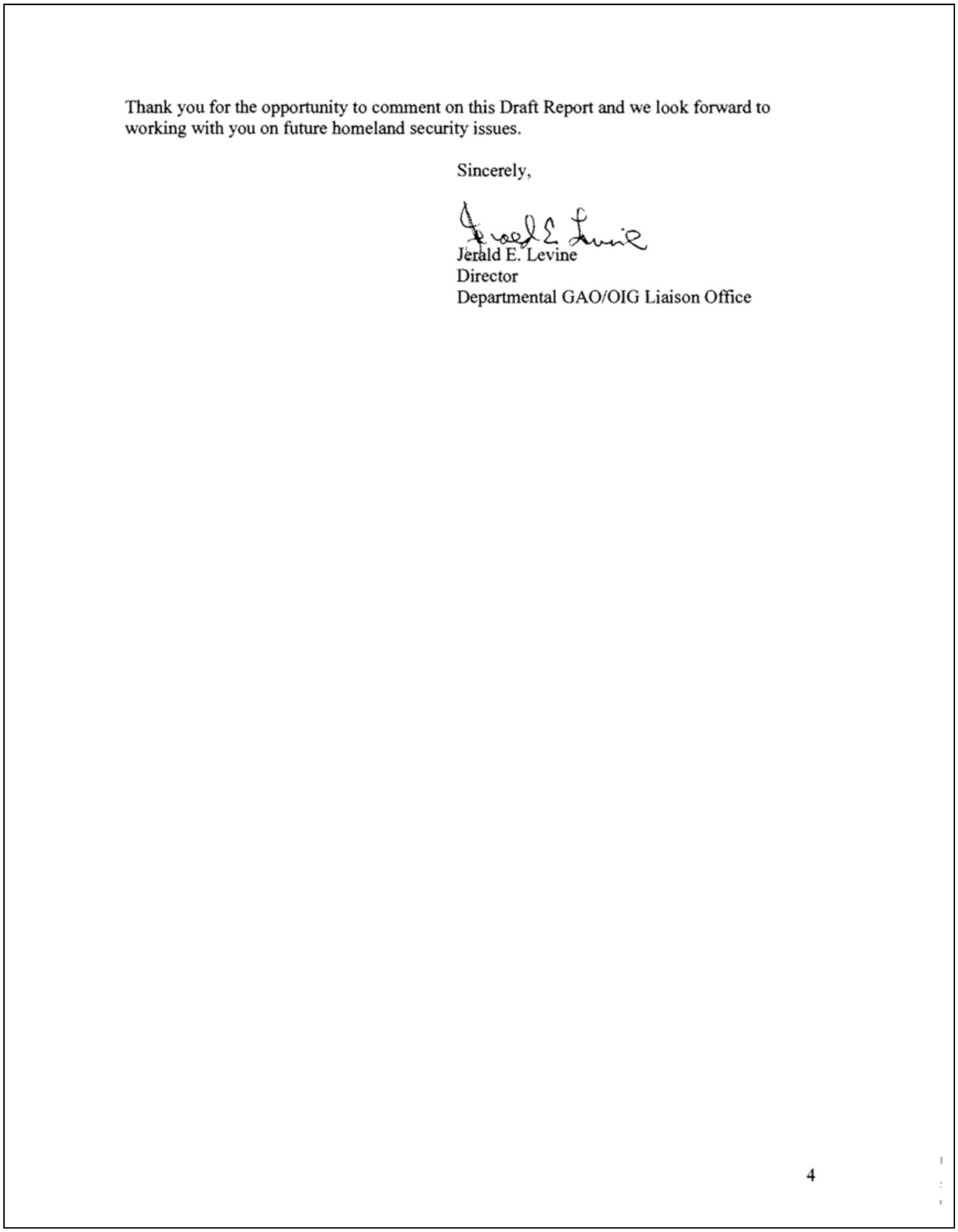
TSA's Response: TSA concurs with this recommendation. In future updates to the Transportation Systems Sector Specific Plan PSD will include performance measures within the Pipeline Modal Annex consistent with the sector format and guidance.

Recommendation 7: To better evaluate PSD's performance in helping strengthen the security of hazardous liquid and natural gas pipelines and improvements in pipeline security, develop additional outcome measures that are directly linked to sector goals and modal objectives and track progress towards its stated pipeline security objective.

TSA's Response: TSA concurs with this recommendation. PSD will develop appropriate outcome measures that reflect the impact of its security programs and the security status of the pipeline industry. In so doing, this effort will be made consistent with the performance measurement guidance of the Transportation Systems Sector Specific Plan.

Recommendation 8: To help ensure reliable reporting of security improvements in the pipeline industry, establish reliable baseline data and, until that time, refrain from using reconstructed baseline data to report progress in closing the vulnerability gap.

TSA's Response: TSA concurs with this recommendation. Updated data from repeat Corporate Security Reviews will be utilized to insure more accurate reporting of the pipeline industry's security status.



Thank you for the opportunity to comment on this Draft Report and we look forward to working with you on future homeland security issues.

Sincerely,

Jerald E. Levine

Jerald E. Levine
Director
Departmental GAO/OIG Liaison Office

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Stephen M. Lord (202) 512-4379 or lords@gao.gov

Acknowledgments

In addition to the contact named above, Edward J. George, Jr., Assistant Director, and Lori A. Weiss, Analyst-in-Charge, managed this assignment. Valerie Kasindi and Jaclyn Nelson made significant contributions to the work. Chuck Bausell, Jr. provided expertise on risk management, David Bruno provided expertise on transportation security issues, and Mark Gaffigan provided expertise on energy issues. Tracey King provided legal support. Michele Fejfar and Amanda Miller assisted with design, methodology, and data analysis. Christopher Currie, Debra Sebastian, and Adam Vogt provided assistance in report preparation and Lydia Araya developed the report's graphics.

(440768)

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 Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to 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 Web site, http://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.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@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

Please Print on Recycled Paper