

Annex F: Pipeline



Contents

1. Executive Summary	315
2. Pipeline Overview	317
2.1 Pipeline Mode Description	317
2.2 Assets, Systems and Networks	317
2.3 Risk Profile (Threats to Pipelines)	318
2.4 Sector Partners and Information-Sharing Mechanisms	319
2.4.1 Federal Agencies Responsible for Pipelines	319
2.4.2 Information Sharing	319
3. Implementation Plan	321
3.1 Goals, Objectives, and Programs/Projects/Activities	321
3.1.1 Transportation Systems Sector Goals	321
3.1.2 Pipeline Modal Objectives	322
3.1.3 Pipeline Modal Supporting Strategies	322
3.2 Strategic Risk	323
3.3 Operational Risk	323
3.4 Decisionmaking Factors	324
3.5 Risk Mitigation Pipeline Activities, Programs, and Projects	325
3.5.1 TSA-Led Programs, Projects, and Activities	325
3.5.2 Other Federal Agency-Led Programs, Projects, and Activities	327
3.5.3 Pipeline Industry-Led Programs, Projects, and Activities	328
3.5.4 Industry Smart Practices, Guidelines, Standards, and Programs	329
3.6 Metrics	329
4. Security Gaps	331
5. Way Forward	333
Appendix 1. Objectives/Strategies/Programs/Goals Alignment Table	335

List of Figures

Figure F2-1:Oil and Gas Movement to Market	318
Figure F3-1:Goals, Objectives, and Strategies Alignment	321
Figure F3-2:Risk Definition Framework	324



1. Executive Summary

Each day, thousands of businesses and millions of people rely on the safe, secure, and efficient movement of commodities through the transportation system. Manmade or natural disruptions to this critical system could result in significant harm to the social and economic well-being of the country. The Nation's pipeline system is a mode of transportation with unique infrastructure security characteristics and requirements.

As required by Executive Order 13416,¹ the Pipeline Modal Annex implements the Transportation Systems Sector-Specific Plan (SSP) and was developed to ensure the security and resiliency of the pipeline mode.

The vision of this plan is to ensure that the pipeline mode is secure, resilient, and able to quickly detect physical and cyber intrusions or attacks, mitigate the adverse consequences of an incident, and quickly restore pipeline service. A robust nationwide pipeline security program will instill public confidence in the reliability of the Nation's critical energy infrastructure, enhance public safety, and ensure the continued functioning of other critical infrastructure sectors that depend on secure and reliable supplies of products for consumption.

The SSP and the Pipeline Modal Annex were developed, reviewed, and updated using both the Transportation Systems Sector and the Energy Sector Government Coordinating Council (GCC) and Sector Coordinating Council (SCC) frameworks. The draft plans were distributed to the pipeline industry via the GCC and SCC memberships for another level of review and input before finalizing the documents.

The Transportation Security Administration (TSA) Pipeline Security Division will work with its security partners in both the Transportation Systems and Energy Sectors to update the Transportation Systems SSP and Pipeline Modal Annex regularly, as called for in the National Infrastructure Protection Plan (NIPP) and Executive Order 13416. The updating process is a responsibility shared with pipeline partners collaboratively through the GCC/SCC/Critical Infrastructure Partnership Advisory Council (CIPAC) framework.

The core of the plan is the TSA pipeline system relative risk assessment and prioritization methodology. This methodology provides a logical prioritization process to systematically list, analyze, and sort pipeline systems. By prioritization, security resources can be effectively used to manage risk mitigation in order to protect critical pipelines from threats. The methodology is based on the Transportation Systems Sector Risk Management Framework methodology, which is, in turn, based on the risk management framework presented in the NIPP.

¹ *Strengthening Surface Transportation Security*, December 5, 2006.

With a view toward this future-state, the SSP and this Pipeline Modal Annex specifically focus on how the Pipeline Security Division within the Transportation Systems Sector will continue to enhance the security of its critical infrastructure and key resources (CIKR).

The Pipeline Security programs developed to protect the Nation's pipeline system(s) are key to making the nation safer, more secure, and more resilient in the face of all hazards.

2. Pipeline Overview

2.1 Pipeline Mode Description

The Nation's pipeline system is a mode of transportation with unique infrastructure security characteristics and requirements. Vast networks of pipelines traverse hundreds of thousands of miles to transport nearly all of the natural gas and about 65 percent of hazardous liquids, including crude and refined petroleum products, consumed within the United States. Pipelines are an efficient and fundamentally safe means of transportation. However, pipelines also transport hydrocarbons that can potentially cause deaths and injuries to the general public, and/or inflict damage to the environment. Most pipelines are privately owned and operated, and with rare exceptions, are buried underground. The pipeline industry's current security posture is based on voluntary guidelines that were developed, issued, and implemented through a collaborative effort between the Federal government and industry associations.

2.2 Assets, Systems and Networks

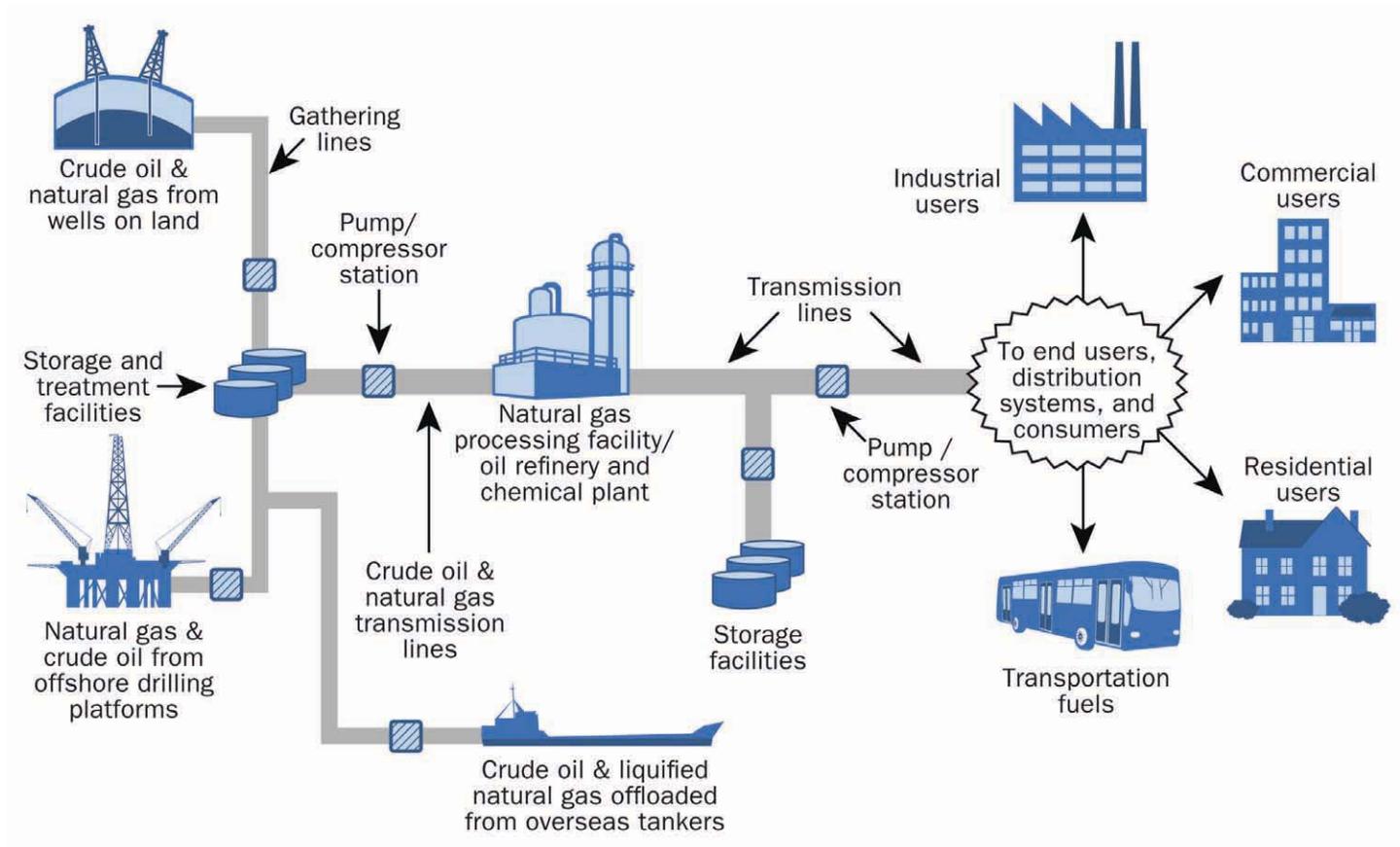
The following are the main types of pipelines:²

1. **Natural Gas Transmission and Storage.** These lines are mostly interstate, transporting natural gas over 320,500 miles of pipelines from sources to communities, operated by more than 700 operators. More than 400 natural gas storage facilities are in the United States.
2. **Hazardous Liquid Pipelines and Tanks.** These pipelines predominately consist of interstate pipelines transporting crude oil to refineries and refined petroleum products (e.g., fuels) to marketing terminals and airports; they carry diesel fuel, gasoline, jet fuel, anhydrous ammonia, and carbon dioxide to product terminals and airports. Nationwide, there are about 168,900 miles of these pipelines in operation, operated by more than 200 operators.
3. **Natural Gas Distribution.** These are typically local distribution company pipelines, mostly intrastate, that transport natural gas from transmission pipelines to residential, commercial, and industrial customers. Included in this segment of the industry are the local distribution companies, i.e., natural gas utilities. More than 1,300 operators operate approximately 2.2 million miles of natural gas distribution pipelines nationwide.
4. **Liquefied Natural Gas (LNG) Processing and Storage Facilities.** More than 109 facilities nationwide either directly receive LNG from tanks, ships, or trucks, or receive natural gas via pipeline for processing (liquefying) into LNG and then store it on site in specialized tanks. When needed, LNG is vaporized for injection into natural gas pipeline systems.

² The following sources were used for information in this section: DOT Bureau of Transportation Statistics; DOT Office of Pipeline Safety; Association of Oil Pipelines; American Gas Association; American Public Gas Association; and Interstate Natural Gas Association of America.

Figure F2-1 shows the structure of oil and gas pipeline system movement to market.

Figure F2-1: Oil and Gas Movement to Market



2.3 Risk Profile (Threats to Pipelines)

The pipeline system is a vital part of the U.S. transportation and energy supply, with connections to other critical infrastructure such as airports and power plants. Since the attacks of September 11, 2001, numerous federal warnings have been issued specifically mentioning pipelines as terrorist targets. Many pipelines carry volatile and flammable materials that have the potential to cause serious injury to the public and the environment. The pipeline system is uniquely vulnerable to terrorist attacks because of the products transported, and because pipeline networks are widely dispersed across both remote and urban portions of the country. A pipeline facility could be vandalized or attacked with explosive devices, resulting in flow disruption or the release of its contents.

Pipelines are also susceptible to cyber attacks on their computer control systems. Cyber threats could result from the acts of a terrorist-hacker, or a rogue employee with computer access. The latter threat requires that specific attention be given to personnel security credentials and access protocols, as well as general cybersecurity protocols. Additionally, attacks on other infrastructure such as regional electricity grids and communication networks could cause a serious disruption in pipeline operations, posing risks for all sectors serviced by pipelines, including the military and major commercial installations.

It is impossible to uniformly protect the pipeline system. While it is difficult to predict what method of attack may be utilized, the risks can be calculated in terms of threat, vulnerability, and consequence, and measures can be taken to safeguard the pipeline system.

American oil pipelines carry over 75 percent of the Nation's crude oil and 60 percent of its refined petroleum products.³ A majority of the Nation's natural gas moves from well to market via pipeline. In addition to oil and natural gas transmission, pipelines are used to transport manufacturing chemicals such as anhydrous ammonia, a critical fertilizer for the American farming industry and feedstock for the chemical industry.

Pipeline disruptions can have effects that ripple through the economy, and at the most extreme, can impact public health and national security. Minor disruptions may result in increased prices of gasoline, diesel fuel, home heating oil, and natural gas. More prolonged disruptions could manifest themselves as widespread energy shortages and the inability to produce products such as plastics, pharmaceuticals, and many chemicals that rely on oil and natural gas as manufacturing feedstock. In the case of an extreme disruption of pipelines, American transportation and manufacturing could be halted, homes could go cold for lack of natural gas or heating oil, and energy for vital defense use may begin to limit American defense capabilities.

2.4 Sector Partners and Information-Sharing Mechanisms

Each of the transportation modes is required to have a GCC. A Pipeline Working Group has been established to address pipeline issues within the Energy Sector GCC. To avoid duplication and eliminate the need for multiple meetings with the same security partners, the Energy Sector GCC Pipeline Working Group also acts as the Pipeline GCC for the Transportation Systems Sector GCC.

The Oil and Natural Gas (ONG) SCC has also established a Pipeline Working Group to address pipelines issues. The ONG SCC Pipeline Working Group also acts as the Pipeline SCC for the Transportation Systems SCC.

The TSA Pipeline Security Division has been a member of the Energy Sector GCC since its inception, and the Department of Energy (DOE) is a member of the Transportation Systems Sector GCC as well. More details on the Energy Sector GCC and ONG SCC can be found in the Energy SSP.

2.4.1 Federal Agencies Responsible for Pipelines

Under the NIPP, TSA is assigned as a Sector-Specific Agency (SSA) for the Transportation Systems Sector, including the pipeline systems mode. The United States Coast Guard is the SSA for the Transportation Systems Sector maritime mode. SSAs are responsible for coordinating infrastructure protection activities within the critical infrastructure sectors. DOE is the SSA for the Energy Sector and therefore works closely with TSA on pipeline security issues, programs, and activities. The Department of Transportation (DOT) is responsible for administering a national program of safety in natural gas and hazardous liquid pipeline transportation, and TSA and DOT collaborate on matters relating to transportation security and transportation infrastructure protection. The Department of Justice through the Federal Bureau of Investigation (FBI) is responsible for investigating and prosecuting actual or attempted attacks on, sabotage of, or disruptions of critical infrastructure in collaboration with the Department of Homeland Security (DHS).

2.4.2 Information Sharing

A number of methods have been employed and will continue to be used to foster good communication and information sharing within the pipeline mode.

³ Bureau of Transportation Statistics (BTS), "National Transportation Statistics," February 2008.

GCC/SCC/CIPAC Framework

The GCC/SCC/CIPAC framework has been and will continue to be used to facilitate discussion and information sharing among pipeline security partners.

TSA Pipeline Security Stakeholder Conference Calls

Since March 2006, the TSA Pipeline Security Division has conducted regular conference calls with pipeline security partners. These conference calls are used to share pipeline security information and educate security partners on many of the programs, activities, and initiatives within the pipeline mode or within the Transportation Systems Sector. These conference calls also provide pipeline security partners with the opportunity to ask questions and bring up other important issues for discussion. Ad-hoc stakeholder conference calls can be conducted on short notice as the need arises.

Trade Associations

As appropriate, information is also disseminated through five major trade associations with strong ties to the pipeline industry:

- American Petroleum Institute (API),
- Association of Oil Pipe Lines (AOPL),
- American Public Gas Association (APGA),
- Interstate Natural Gas Association of America (INGAA), and
- American Gas Association (AGA).

These associations can quickly pass information to their member companies, as demonstrated by the numerous information-sharing sessions through conference calls they have conducted with their respective security committees over the past eight years.

Homeland Security Information Network

The Homeland Security Information Network (HSIN) is an Internet-based communications system DHS established to facilitate exchanging information between DHS and other government, private sector, and non-governmental organizations involved in counterterrorism and incident management activities. In May 2006, the ONG SCC signed a Memorandum of Understanding (MOU) with DHS to establish the ONG HSIN. The TSA Pipeline Security Division communications and information-sharing activities have been incorporated into the ONG HSIN system. There is a link to the TSA Transportation Security Information Sharing and Analysis Center (TS-ISAC) on the ONG HSIN system. Pipeline information can also be found on the TS-ISAC network.

TSA Transportation Suspicious Incident Report

TSA's Office of Intelligence disseminates the Transportation Suspicious Incident Report (TSIR), a weekly unclassified report on all suspicious activity related to transportation. The TSIR includes incident reporting, analyses, images, and graphics on transportation security activities. In addition, select articles focus on security technologies, terrorism, and the challenges of securing the Nation's transportation modes. TSA's Pipeline Security Division shares this weekly report with all interested pipeline security partners in an effort to maintain government transparency and to enhance and improve incident communication and sharing.

Federal Energy Regulatory Commission Pipeline Engineering Data and Damage Reporting

The Federal Energy Regulatory Commission (FERC) has taken steps to provide relevant engineering data that it receives from jurisdictional interstate pipelines in the context of facility siting and permitting to the DOE. In June 2006, the FERC also revised its regulations to require jurisdictional pipelines to report major damage to pipeline systems that result from major disasters, whether they are natural (such as a hurricane) or manmade (such as a terrorist attack). This revision was made, in part, to enhance its ability to provide relevant information to GCC and SCC activities.

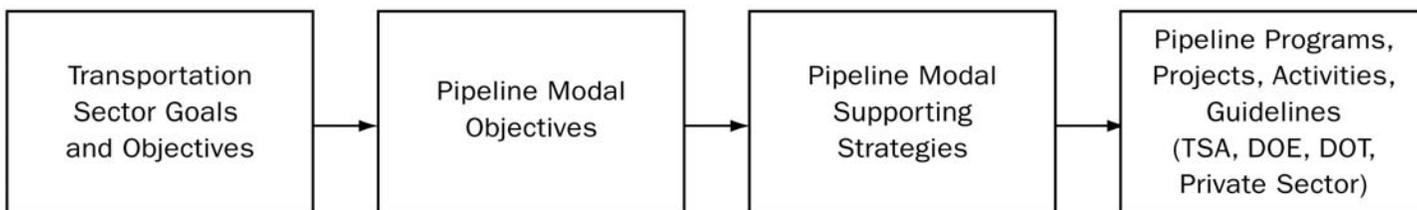
3. Implementation Plan

3.1 Goals, Objectives, and Programs/Projects/Activities

Four overarching Transportation Systems Sector goals and 17 supporting objectives are consistent with the goals outlined in the President’s homeland security agenda, DHS priorities, and the statutory imperatives for protecting the transportation system and improving resiliency of its critical infrastructure and networks (chapter 1, section 1.3 of the Transportation Systems SSP). The Pipeline Modal Annex outlines three objectives that aim to achieve the sector goals within the pipeline transportation domain. Each pipeline modal objective is achieved by a combination of one or more of seven underlying modal strategies. Each of these seven modal strategies is, in turn, supported by programs, projects, and activities. These programs, projects, and activities are the result of the combined contributions of the TSA Pipeline Security Division and other Federal, State, local, and private sector partners and reflect the significant efforts of all pipeline stakeholders to secure our Nation’s pipeline systems.

Figure F3-1 shows the relationships between all goals, objectives, programs, projects, and activities. The sector goals and objectives are supported by the modal objectives; the modal objectives are supported by the strategies, and so on.

Figure F3-1: Goals, Objectives, and Strategies Alignment



The following subsections define the sector goals and objectives, the modal objectives, their supporting strategies, and the programs, projects, and activities. The tables at the end of section 3 provide a specific, detailed description of each modal objective; the strategies, programs, projects, and activities that support it; and the sector goals to which it aligns.

3.1.1 Transportation Systems Sector Goals

The following are the Transportation Systems Sector’s overarching goals:

Goal 1: Prevent and deter acts of terrorism using, or against, the transportation system.

Goal 2: Enhance the all-hazard preparedness and resilience of the global transportation system to safeguard U.S. national interests.

Goal 3: Improve the effective use of resources for transportation security.

Goal 4: Improve sector situational awareness, understanding, and collaboration.

3.1.2 Pipeline Modal Objectives

The three objectives for the Pipeline Modal Annex are as follows:

1. **Reduce level of risk through analysis and implementation of security programs** that enhance deterrence and mitigate critical infrastructure vulnerabilities against threats and natural hazards.
2. **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 natural hazards.
3. **Increase the level of domain awareness, information sharing, response planning, and coordination** through enhanced training, network building, and efficient research and development application.

While no specific objective is directed at achieving “cost-effective use of resources,” where possible each strategy involves maximizing efficient employment of available resources and minimizing duplication of effort. The sector objectives will thereby be supported through the conscious efforts of all stakeholders to make evaluations of cost versus risk and to maximize the use of already available resources.

3.1.3 Pipeline Modal Supporting Strategies

Each modal objective is achieved through a combination of strategies. Each strategy is directly supported by a combination of programs, projects, or activities. These strategies are further described here. The programs, projects, and activities are listed below, along with a brief description and the function and corresponding strategies they support. The following are the modal strategies:

1. Promote the implementation of layered threat deterrence and vulnerability mitigation programs in pipeline systems and critical infrastructure, considering risk analysis and making efficient use of existing resources and minimizing duplication of effort.
2. Develop and perform collaborative risk analysis processes from which mitigation measures and plans are determined using available resources with maximum efficiency.
3. Use collaborative plan development and drill/exercise participation to enhance response, restoration, and recovery capabilities while maximizing efficient use of existing resources and minimizing duplication of effort.
4. Promote pipeline system resiliency and contingency capability enhancement measures that increase pipeline system robustness and resiliency while maximizing efficient use of resources and minimizing duplication of effort.
5. Conduct security-related training that enhances domain awareness of deterrence and mitigation measures, increases knowledge of response and restores capabilities, and clarifies the roles and responsibilities of all stakeholders within the pipeline domain.
6. Conduct network enhancement and information-sharing activities that promote domain awareness, collaborative planning, and the definition of roles and responsibilities for pipeline security partners.
7. Conduct research and development and other activities that build domain awareness in all facets of risk mitigation and resiliency enhancement through coordinated and efficient use of assets.

3.2 Strategic Risk

This section explains how the pipeline mode participates in data collection for risk assessment.

The TSA Pipeline Security Division gathers data by conducting pipeline Corporate Security Reviews (CSRs) and Critical Facility Inspections (CFIs) in cooperation with sector security partners to further evaluate and categorize pipeline systems.

The CSR program has gathered excellent pipeline system data since its conception in 2003. The CSR program is an on-site security review process with pipeline companies that is used to help establish working relationships with key security representatives. CSRs give TSA an understanding of the pipeline operator's security plan and its implementation. The CSR process uses a standard protocol to capture data on pipeline systems, which can be evaluated both quantitatively and qualitatively to further prioritize critical pipeline systems.

During the CSR process, potentially critical assets are examined and catalogued based on their importance to the pipeline systems. Assets are identified and a link between the asset and the critical pipeline system is then documented. Critical assets include pipeline components, such as the following:

- Pipeline interconnections
- Hubs or market centers
- Metering stations
- Pump stations
- Compressor stations, terminals
- Operation control facilities
- Pipeline bridge crossings
- Critical aboveground piping
- Storage facilities

On August 3, 2007, President Bush signed The Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53 (2007) (9/11 Act). Section 1557 of the law requires TSA, along with DOT, to develop and implement a plan for inspecting the critical facilities of the 100 most critical pipeline systems. The Pipeline Security Division began inspecting the critical facilities in November 2008 and the results of these inspections are used in the data collection process.

3.3 Operational Risk

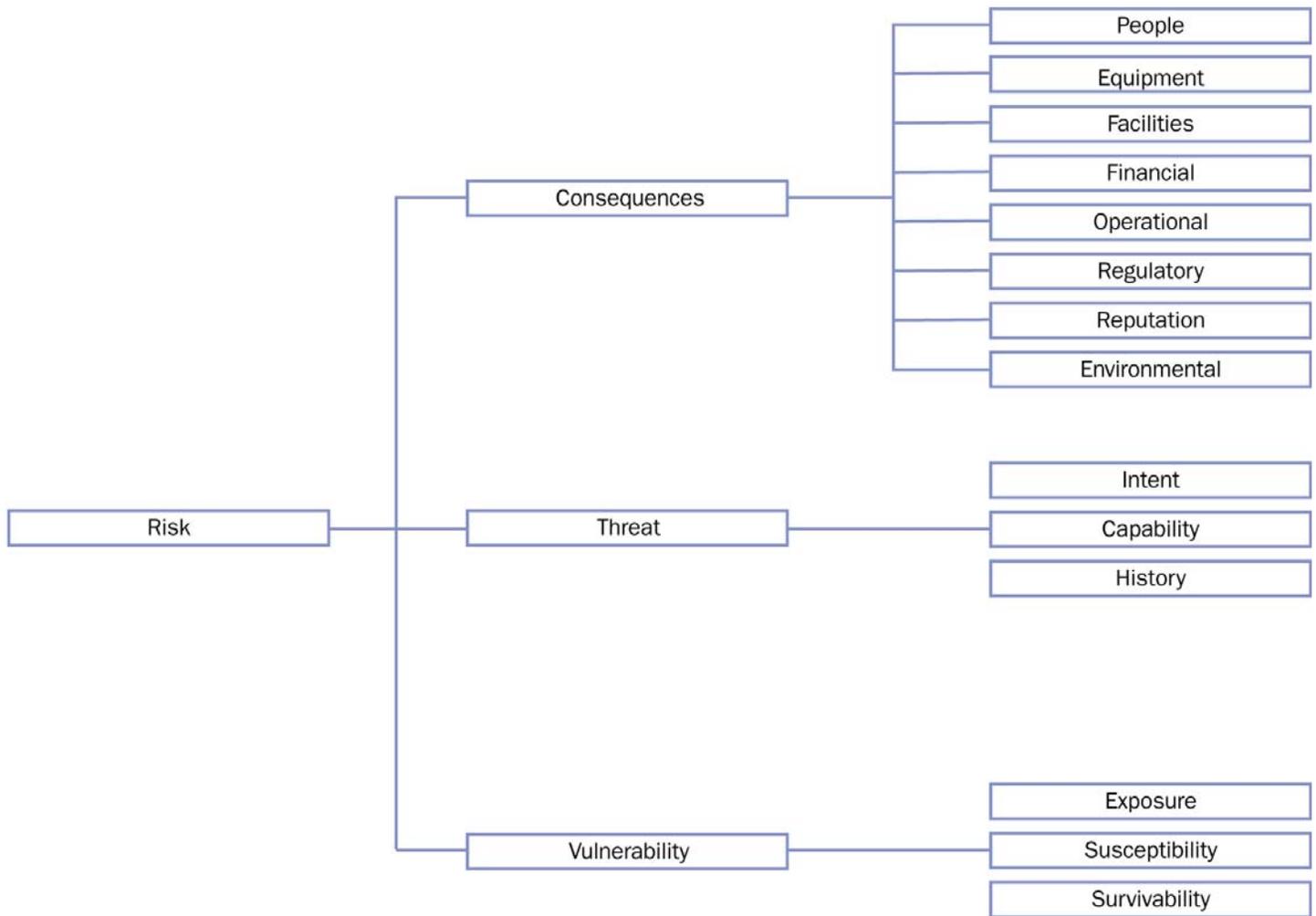
This section explains the pipeline risk assessment method that the TSA Pipeline Security Division utilizes.

In practical terms, a risk-based approach to security is recognizing that there are too many risk scenarios to protect all assets/pipeline/systems equally, so priorities must be established and security resources allocated accordingly. A more theoretical description of risk is that it is a function of likelihood (mathematically expressed as a probability) and consequences (in terms of impact to people or facilities, financial loss, operational disruption, etc.). Likelihood can be further broken down into threat (an adversary's capability and intent) and vulnerability (a target's exposure, susceptibility, survivability).

Measuring risk is a matter of attempting to quantify the various components of it (see above). Some things are, by nature, speculative. For example, one can infer an adversary's intent but not read his or her mind. One must try to measure the various parts of risk for which information is available and make some judgment calls where it is not.

Figure F3-2 shows the framework that will be used to define risk for the purposes of this approach.

Figure F3-2: Risk Definition Framework



Adapted from Patrick Gallagher
 Manager, Group Security Intelligence & Risk, Qantas

The TSA Pipeline Security Division relies on TSA’s Office of Intelligence to provide threat assessments based on information received from the Intelligence Community: the FBI, Central Intelligence Agency, DHS Office of Intelligence and Analysis, and others.

The TSA Pipeline Security Division uses the results of the CSRs and the CFIs, the pipeline’s energy throughput, and the threat as indicators of the security risk in the pipeline industry measured by the formula $R = f(T, V, C)$. The measurable risk is the difference between the desired state and the current state using the Pipeline CSR results (V), the energy throughput (C), and the threat (T).

3.4 Decisionmaking Factors

This section explains the TSA Pipeline Security Division’s methods for identifying pipeline modal priorities utilizing the results from the CSRs, the CFIs, and other applicable information.

The natural gas and hazardous liquids pipeline system infrastructure is substantial, widely dispersed, and mostly privately-owned. While there is a desire to secure all aspects of all critical infrastructure, the total pipeline system cannot be given equal oversight, protection, focus, or security resources. Therefore, appropriate resources must be focused where they are needed the most.

A Pipeline System Relative Risk Ranking Tool that provides a logical prioritization process is required to list systematically, analyze, and sort pipeline systems and critical pipeline components within those pipeline systems. The TSA Pipeline Security Division will implement the prioritization process with input from pipeline operators and industry trade associations. Through prioritization, security resources can be used effectively for risk management to protect critical pipelines from all hazards. Pipeline systems will always be ranked and evaluated first before any specific asset or component. The overall guidance for the methodology is introduced in chapter 3 of the Transportation Systems SSP.

Individual pipeline companies conduct security risk analyses on their corporate assets. Reasonable resources should be allocated as necessary to ensure an appropriate level of security. During the CSR process, the TSA Pipeline Security Division will verify that the company's risk analysis is being conducted and reasonable actions taken.

In the first step, the TSA Pipeline Security Division will use quantitative methods to sort and provide a rough screening of more than 2,200 pipeline systems throughout the United States. Hazardous liquids, natural gas distribution, and transmission systems will be sorted by the total equivalent energy transported, typically converted to therms per year. The higher the throughput in therms (i.e., energy delivered to end users), the higher the pipeline system will be sorted on the list. The logic is that systems with higher annual energy shipment are more valuable to the Nation's energy security. In this manner, the total universe of pipeline systems will be pared down to a small finite number for further evaluation in the next steps. Qualitative methods from subject matter experts will also be used where applicable to consider the criticality of certain systems that quantitative methods do not adequately address.

TSA will use the Pipeline System Relative Risk Ranking Tool to rank the most critical systems and assets according to the greatest importance to energy supplies and risk, in threat, vulnerability, and consequences. The list will be sorted using proven qualitative and quantitative methods. A subject matter ranking factor (percentage adding to 100 percent) will weigh the importance on the highest areas of concern.

Using the methodology described above, the algorithm will generate a unit-less relative risk score. The higher the score, the higher the pipeline will be in the relative risk ranking. The algorithm will factor in countermeasures as a negative number, reducing the risk score. With periodic reevaluation, the ranking will probably change over time. In addition, subject matter experts will use their knowledge to verify the algorithm's results.

3.5 Risk Mitigation Pipeline Activities, Programs, and Projects

The tables in sections 3.5.1, 3.5.2, and 3.5.3 present the programs, projects, and activities (either already undertaken or planned) that promote prevention, deterrence, preparedness, system resiliency, and information for physical, human, and cyber threats within the pipeline system domain. Moreover, many programs strengthen partnerships and build security networks that extend internationally as well. These sections are divided into TSA-led efforts, efforts led by other Federal agencies or departments, and pipeline industry initiatives. The tables list the programs, provide a brief description of each, list the participating organizations, and note the pipeline modal strategies each program supports.

3.5.1 TSA-Led Programs, Projects, and Activities

The TSA Pipeline Security Division has numerous programs, projects, and activities designed to increase the security of the Nation's pipeline systems. The cornerstones of these programs are the Pipeline System Relative Risk Ranking and Prioritization Tool and the Pipeline CSR programs.

Program/Project/ Activity	Description	Participants	Pipeline Strategies Supported
Pipeline System Relative Risk Tool	This program and associated activities compile statistical data from CSRs, CFIs, and other data sources on pipeline systems to perform a relative risk ranking.	TSA, Industry	2, 7
Pipeline CSR Program	Since 2003, TSA has been conducting CSRs, an on-site security review, with pipeline companies to help establish working relationships with key security representatives in the pipeline industry as well as provide TSA with a general understanding of a pipeline operator's security planning and implementation.	TSA, Industry	1, 6
Pipeline CFI Program	On August 3, 2007, President Bush signed the 9/11 Act. Section 1557 of the law requires TSA, along with DOT, to develop and implement a plan for inspecting the critical facilities of the 100 most critical pipeline systems. The Pipeline Security Division began inspecting the critical facilities in November 2008.	TSA, Industry	1, 6
Revision of the Pipeline Security Guidelines	In 2002, DOT's Office of Pipeline Safety issued pipeline security guidelines to improve the security posture of the pipeline industry. TSA has widely accepted these guidelines and conducts CSRs of pipeline operators based on these guidelines. After the DOT guidelines were published, TSA was designated in the NIPP as the SSA responsible for pipeline security. As such, the responsibility for revising the guidelines lies with TSA. TSA is in the final process of updating those guidelines, with input from government and industry partners.	TSA, Other Government Agencies, Industry	1,2,3,4,5,6
Pipeline Security Incident and Recovery Protocol Plan	In the 9/11 Act, Section 1558 tasked the Secretary of Homeland Security (TSA) and the Secretary of the DOT Pipeline Hazardous Materials Safety Administration (PHMSA) to develop a Pipeline Security and Incident Recovery Plan and to submit that plan to Congress. The Pipeline Security Division, in collaboration with PHMSA, government and industry partners has completed the plan.	TSA, Other Government Agencies, Industry	1,2,3,4,5,6
TIH Materials Transmitted in Pipelines	In addition to oil and natural gas, pipelines are also used to transmit hazardous materials. This program will address the potential risks associated to the transport of these materials.	TSA, Government Partners, Industry	1,3,5,7
Pipeline Cross- Border Vulnerability Assessment Program (International)	The pipeline cross-border vulnerability assessments are in support of the Smart Border Accord and the Security and Prosperity Partnership Agreement. Assessment teams of Canadian and U.S. subject matter experts in pipeline operations, control systems, infrastructure interdependencies, and assault planning visit critical cross-border pipeline infrastructure, identify security gaps, and recommend protective measures to mitigate those gaps.	TSA, Natural Resources Canada	1, 2, 5

Program/Project/Activity	Description	Participants	Pipeline Strategies Supported
International Pipeline Security Forum	International forum for U.S. and Canadian Governments and industry pipeline officials to discuss security issues and topics.	TSA, Natural Resources Canada, Government Agencies, Industry	5, 6
Pipeline Exercises, The Intermodal Security Training Exercise Program (I-STEP)	The I-STEP program promoting security partner awareness and involvement, encourages security partner participation in program development, ensures program alignment with national standards and requirements, conducts exercises relevant to security partners' challenges and risks and refines the program through evaluation and continuous improvement.	TSA, Government Partners, Industry	1,2,3,4,5,6,7
Training Materials	Informational CDs about pipeline security issues and improvised explosive devices (IED).	TSA	1, 2, 6
TSA Pipeline Security Stakeholder Conference Calls	Periodic information-sharing teleconference calls between TSA, other government agencies, and industry security partners.	TSA, Other Government Agencies, Industry	6
Transportation Systems GCC, Energy GCC and CIPAC Joint Sector Committee	Government security partners participate in GCCs and CIPAC to coordinate interagency and cross-jurisdictional implementation of security for critical infrastructure.	TSA, DOE, Government Agencies, Industry	6
Pipeline Security Smart Practices	Document to assist hazardous liquid and natural gas pipeline industries in their security planning and implementation.	TSA, Industry	1,4

3.5.2 Other Federal Agency-Led Programs, Projects, and Activities

Program/Project/Activity	Description	Participants	Pipeline Strategies Supported
Homeland Security Information Network (HSIN)	Internet-based communications system and information-sharing tool providing security information, threat intelligence, indications, and warnings.	DHS, TSA, DOE, Industry	6
Homeland Security Advisory System (HSAS)	Information-sharing program that makes government, the private sector, and the public more vigilant when credible threat is identified.	DHS	1, 6
DOT, DOE, DHS Incident Drill Programs/ Sponsorship and Participation	Tabletop and field exercise facilitation.	DOT, DOE, DHS, PHMSA	3, 4

3.5.3 Pipeline Industry-Led Programs, Projects, and Activities

The pipeline industry has been effective in its prevention, deterrence, preparedness, system resiliency, and information-sharing efforts. The following examples are a small sample of the industry's programs, projects, and activities that support the pipeline modal objectives.

Program/Project/ Activity	Description	Participants	Pipeline Strategies Supported
ONG/Pipeline SCC and CIPAC Joint Sector Committee	Private-sector companies participate in the SCC and CIPAC to engage with industry and government security partners in critical infrastructure protection discussions and activities.	Industry, Government Agencies	6
Pipeline Company-Based Drill/Exercise Initiatives and Participation	Private-sector companies participate in drills/exercises related to infrastructure security at all levels (Federal, State, regional, local, and corporate); companies have engaged in tabletop and on-site simulated exercises.	Pipeline Companies	3
Pipeline Company-Based Training Initiatives	Training initiatives include corporate and field training and usually include response measures tied to the DHS Threat Advisory System; tools include briefings, manuals, CDs, and computer-based training.	Pipeline Companies	5
API/NPRA Security Vulnerability Assessment for the Petroleum and Petrochemical Industries	Provides practical knowledge for performing security vulnerability assessments in multiple petroleum and petrochemical-related industries.	API, NPRA	2
API Security Committee and AGA Security Committee-Sponsored Training and Workshops	Workshops/forums and training for gas and liquid petroleum industry.	API	5, 6
Pipeline Company Security Protective and Deterrence Measures	Pipeline operators enhance protective and deterrence measures in accordance with Pipeline Security Circular 2002.	Pipeline Companies	1

3.5.4 Industry Smart Practices, Guidelines, Standards, and Programs

Practices/ Guidelines/ Standards/Program	Description	Participants	Pipeline Strategies Supported
Security Guidelines; Natural Gas Industry, Transmission and Distribution: Assessment Guidelines	Provide an approach for vulnerability assessment, critical facility definition, detection/deterrence methods, response and recovery, cybersecurity, and relevant operational standards.	AGA, INGAA, and APGA	1
Cryptographic Protection of Supervisory Control and Data Acquisition (SCADA) Communications	Define encryption methods for SCADA systems.	AGA	1
API Security in the Petroleum Industry: Practices Guidelines	Recommend security practices for all segments of liquid and gas petroleum.	API	2
API Pipeline SCADA Security Standard (API Standard 1164)	Provide a model for proactive industry actions to improve the security of the Nation's energy infrastructure.	API	1
API Information Management and Technology Program	Provide a comprehensive review and quantitative assessment of company security programs.	API	2

3.6 Metrics

To quantify and establish a pipeline risk reduction metric, the TSA Pipeline Security Division uses the results of the CSRs and the CFIs, the pipeline's energy throughput, and the threat as indicators of the security risk in the pipeline industry measured by the formula $R = f(T, V, C)$. The measurable risk is the difference between the desired state and the current state using the Pipeline CSR results (V), the energy throughput (C), and (T).



4. Security Gaps

The TSA Pipeline Security Division has conducted CSRs since 2003 and began conducting CFIs in 2008. Utilizing the data obtained in those programs and other data resources, the following security gaps and risk mitigation activities and programs have been developed or are under development.

1. Cross-border (international) pipelines are becoming increasingly important to the Nation's pipeline industry. Action Item 21 of the Smart Border Accord requires that the United States and Canada conduct joint assessments on trans-border infrastructure and identify necessary additional protective measures. In the area of pipeline security, TSA has partnered with Natural Resources Canada to conduct system assessments. Six pipeline systems have been reviewed by a joint U.S./Canadian team. The assessments will continue with Canada.
2. Security awareness training is inconsistent throughout the pipeline industry. To address this gap, one of the programs and objectives of the TSA Pipeline Security Division is the development of training CDs and other training materials. The objective of this project is to assist the pipeline industry in achieving desired levels of security through increased knowledge of effective security measures and heightened awareness of vulnerabilities, potential threats, and targets.
3. In addition to oil and natural gas, pipelines are also used to transmit TIH materials. These pipelines have proven to be potential threats and the products present a serious hazard if released. This program will address the potential risks associated to these pipelines and assist the operators with the development of security programs.
4. Security drills and exercise programs are also inconsistent throughout the pipeline industry. To address these gaps, the TSA Pipeline Security Program is developing a pipeline security exercise program in coordination with the pipeline industry and the TSA I-STEP. The I-STEP program promotes security partner awareness and involvement, encourages security partner participation in program development, ensures program alignment with national standards and requirements, conducts exercises relevant to security partners' challenges and risks, and refines the program through evaluation and continuous improvement.

Also, the TSA Pipeline Security Program is coordinating with the Visible Intermodal Prevention and Response (VIPR) teams. VIPR teams are comprised of a variety of personnel drawn from TSA's Federal Air Marshal Service (FAMS), Transportation Security Inspectors, as well as state and local law enforcement (among others). The actual team composition for each VIPR operation is determined collectively by the participating organizations as part of the process of developing a deployment operations plan.

VIPRs, when randomly deployed, can serve as a deterrent, providing a highly visible law enforcement presence at critical pipeline facilities. VIPR operations can disrupt a potential attacker's planning process and give the impression that a facility is too well-protected to be attacked, forcing an attacker to shift his focus elsewhere. In the case of a specific threat to a pipeline facility or system, deploying VIPR teams to protect critical facilities can be a valuable tool to defend key assets. In the case of unmanned facilities, VIPR operations can be conducted covertly, in a counter-surveillance effort. This approach

can be particularly useful if there is a specific threat but the authorities do not want to disclose to the attacker that they have been discovered.

5. In 2002, DOT's Office of Pipeline Safety issued pipeline security guidelines to improve the security posture of the pipeline industry. TSA has widely accepted these guidelines and conducts CSRs of pipeline operators based on these guidelines. After the DOT guidelines were published, TSA was designated in the NIPP as the SSA responsible for pipeline security. TSA, in coordination and collaboration with government and industry partners is in the process of updating the guidelines.
6. The "Pipeline Security Smart Practices" reflect the application of data collected from CSRs conducted since the inception of the program in the fall of 2003. A qualitative and quantitative examination of this data, coupled with literature research of pipeline security measures, identified smart practices operators can institute to promote an effective security program. The practices cover a range of topical security areas, including risk and vulnerability assessments, security planning, threat information, employment screening, facility access controls, physical security, intrusion detection, monitoring systems, SCADA and information technology security, awareness training, incident management planning, drills and exercises, and cooperation with regional and local partners, such as law enforcement and other pipeline operators.
7. In recognition of the need to effectively communicate information pertaining to pipeline incidents, and to synchronize a response among the relevant federal agencies, DHS/TSA and DOT/PHMSA established the Interagency Threat Coordination Committee (ITCC) during the development of the Pipeline Incident and Recovery Plan. The ITCC is designed to organize and communicate developing threat information among federal agencies that may have responsibilities during a pipeline incident response. The ITCC will communicate information at the headquarters level, so the development of Federal action plans can be implemented in a coordinated fashion while avoiding overlap or a duplication of effort. The ITCC will also work to identify any type of assistance that may be useful to owners/operators and provide subject matter information from Federal experts concerning the threat.

5. Way Forward

The TSA Pipeline Security Division will continue to participate in all aforementioned programs, projects, and activities. In addition, the TSA Pipeline Security Division plans to address needed improvements and gaps in the following areas to improve security awareness.

In-Depth Pipeline Assessments – TSA plans to conduct more detailed system and asset assessment programs. Private pipeline operators will have the chance to review and provide input to these assessment programs as well. It is also recommended that pipeline operators conduct detailed system assessments of their critical pipeline systems. In this advanced assessment, TSA and pipeline operators will first assess in greater detail the pipeline systems. The assessment evaluates vulnerabilities and develops mitigation options and countermeasures. Vulnerabilities are the characteristics of a network's, system's, or asset's design, location, security posture, process, or operation that render it susceptible to destruction, incapacitation, or exploitation by mechanical failures, natural hazards, terrorist attacks, or other malicious acts.

The system assessment will evaluate physical security, operations, and processes in a more detailed way than is possible with the current CSR program. Pipeline systems will be evaluated based on how many other operators serve their market areas and on their operational integrity, redundancy, and resilience to attack. The assessment will also examine the impacts of prolonged system downtime and the operator's ability to repair and recover from an attack. The economic and environmental consequences of a system failure will be projected. An operator's corporate security, continuity of operations, disaster recovery plans, and mutual aid arrangements will be evaluated in detail. TSA will assess an operator's ability to recover rapidly, based on supply chain, material, equipment, and manpower resources. TSA will assess the supplies of the commodities the pipeline transported and the availability of alternate sources of supply, the availability of emergency storage, and delivery capabilities. The operator's control processes and control center will be evaluated, as well as cybersecurity for SCADA systems. Communications and management control systems and interdependency with other suppliers and utilities will also be evaluated.

In the future, TSA will assess in greater detail the pipeline assets. The main types of assessments will be facilitated, Federal-led assessments and/or owner-operator self-assessments. In either case, assessors will evaluate existing security measures, vulnerabilities, consequences, and threats. Currently, no single assessment methodology is universally applicable to all system components or assets. A wide variety of tools are currently in use and each varies in assessment approach. As outlined in the NIPP, flexibility on the approaches taken is given as long as it conforms to the NIPP's basic criteria.

Pipeline Security Training – As noted in the Security Gaps section, security awareness training is inconsistent throughout the pipeline industry. To address this gap, one of the programs and objectives of the TSA Pipeline Security Division is the development of training CDs and other training materials. The objective of this project is to assist the pipeline industry in achieving desired levels of security through increased knowledge of effective security measures and heightened awareness of vulnerabilities, potential threats, and targets. TSA has developed a 30-minute training DVD that is tailored specifically to an audience

of pipeline operators. The training covers topics such as security measures, awareness of vulnerabilities, potential threats, and targeting. A second training CD addresses the IED threat to pipelines.

Pipeline Transmission of Hazardous Materials – As noted in the Security Gaps section, pipelines are also used to transmit TIH materials. These pipelines have proven to be potential threats as the products present a serious hazard if released. This program will address the potential risks associated with these pipelines and assist the operators with the development of security programs. Plans are to expand this program in FY 2011 with the addition of resources to the Pipeline Security Division.

Security Drills and Exercises – The TSA Pipeline Security Division is developing a pipeline security exercise program in coordination with the pipeline industry, the TSA I-STEP and the TSA VIPR teams. The first exercise was conducted in October 2009 and the plan is to conduct at least two exercises per year.

Pipeline Security Guidelines and Regulations – The TSA Pipeline Security Division in coordination and collaboration with government and industry partners updated the pipeline security guidelines and planned to issue these guidelines in FY 2010. Section 1557 of the 9/11 Act notes that, if it is determined that regulations are appropriate to reduce risk and apply appropriate mitigation procedures, regulations shall be promulgated and necessary inspection and enforcement actions be developed.

Pipeline Incident Recovery Plan – In the 9/11 Act, Section 1558 of the Act tasked the Secretary of Homeland Security (TSA) and the Secretary of the Department of Transportation (PHMSA) to develop a Pipeline Security and Incident Recovery Plan and to submit that plan to Congress. The Pipeline Security Division in cooperation with PHMSA, government and industry partners has completed the plan and submitted the plan to Congress.⁴

⁴ A copy of the plan can be found at http://www.tsa.gov/what_we_do/tsnm/pipelines/resources.shtml.

Appendix 1. Objectives/ Strategies/ Programs/ Goals Alignment Table

Pipeline Modal Objectives	Supporting Strategies	Supporting Programs, Projects, Activities, Guidelines, etc.	SSP Goals Supported
1. Reduce level of risk through analysis and implementation of security programs that enhance deterrence and mitigate critical infrastructure vulnerabilities against threats and natural disasters.	1. Implement layered threat deterrence and vulnerability mitigation programs	<ul style="list-style-type: none"> • Pipeline Cross Border Vulnerability Assessment Program • Pipeline Corporate Security Review (CSR) Program • CFI Program • Security Awareness Training CD • Pipeline Security Smart Practices • Pipeline Transmission of TIH Materials 	<ol style="list-style-type: none"> 1. Prevent and deter acts of terrorism using, or against, the transportation system. 2. Enhance the all-hazard preparedness and resilience of the global transportation system to safeguard U.S. national interests. 3. Improve the effective use of resources for transportation security. 4. Improve sector situational awareness, understanding, and collaboration.
	2. Develop and perform collaborative risk analysis processes	<ul style="list-style-type: none"> • Pipeline Cross-Border Vulnerability Assessment Program • Pipeline System Relative Risk Tool 	
2. 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 disasters.	3. Use collaborative plan development and drill/exercise participation	<ul style="list-style-type: none"> • Company Based Drill/Exercises Participation • TSA Drills and Exercises • Pipeline Security Incident and Recovery Plan 	<ol style="list-style-type: none"> 1. Prevent and deter acts of terrorism using, or against, the transportation system. 2. Enhance the all-hazard preparedness and resilience of the global transportation system to safeguard U.S. national interests. 3. Improve the effective use of resources for transportation security. 4. Improve sector situational awareness, understanding, and collaboration.
	4. Promote pipeline system resilience and contingency capability enhancement measures	<ul style="list-style-type: none"> • Company Based Drill/Exercises Participation • TSA Drills and Exercises • Pipeline Security Incident and Recovery Plan • Pipeline Policy and Planning 	
	5. Conduct security-related training that enhances domain awareness	<ul style="list-style-type: none"> • TSA Pipeline Security Training Programs 	

Pipeline Modal Objectives	Supporting Strategies	Supporting Programs, Projects, Activities, Guidelines, etc.	SSP Goals Supported
<p>3. Increase the level of domain awareness, information-sharing, and response planning and coordination through enhanced training, network building, and efficient research, development application.</p>	<p>5. Conduct security-related training that enhances domain awareness</p>	<ul style="list-style-type: none"> • DOT-sponsored Contingency, Resiliency, Response, Restore Training/Workshops • TSA Pipeline Security Awareness Training CD • API/AGA Workshops 	<ol style="list-style-type: none"> 1. Prevent and deter acts of terrorism using, or against, the transportation system. 2. Enhance the all-hazard preparedness and resilience of the global transportation system to safeguard U.S. national interests. 3. Improve the effective use of resources for transportation security. 4. Improve sector situational awareness, understanding, and collaboration.
	<p>6. Conduct network enhancement and information-sharing activities</p>	<ul style="list-style-type: none"> • Pipeline Cross Border Vulnerability Assessment Program • CSR Program • CFI Program • International Pipeline Security Forum • Pipeline Policy and Planning • Security Awareness Training CDs • Pipeline Security Smart Practices • TSA Pipeline Security Stakeholder Conference Calls • Pipeline Company-Based Security Training Initiatives 	
	<p>7. Conduct research and development and other activities that build domain awareness</p>	<ul style="list-style-type: none"> • Relative Risk Ranking Tool 	

