Pipeline Modal
Annex

Table of Contents
Pipeline Modal Annex

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, the Pipeline Modal Annex implements the Transportation Sector Specific Plan (TSSP) and was developed to ensure the security and resiliency of the pipeline sector. The vision of this plan is to ensure that the pipeline sector is secure, resilient, and able to quickly detect physical and cyber intrusion or attack, mitigate the adverse consequences of an incident, and quickly restore pipeline service.

The TSSP and the Pipeline Modal Annex were developed, reviewed, and updated using both the Transportation Sector and the Energy Sector Government Coordinating Council (GCC) and Sector Coordinating Council (SCC) frameworks. In accordance with the National Infrastructure Protection Plan (NIPP), a Critical Infrastructure Partnership Advisory Council (CIPAC) Oil and Natural Gas (ONG) Joint Sector Committee was established to provide a legal framework for members of the Energy Sector GCC and ONG SCC to engage in joint critical infrastructure protection discussions and activities, including those involved with pipeline security. Under this CIPAC committee, a Pipeline Working Group writing team was formed to develop and review applicable Sector-Specific Plans (SSPs), including the Energy SSP and the TSSP. The writing team reviewed and commented on the draft TSSP Base Plan and drafted the Pipeline Modal Annex. 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.

TSA will work with its security partners in both the transportation and energy sectors to update the TSSP and Pipeline Modal Annex regularly, as called for in the NIPP and Executive Order. The updating process is a responsibility shared with pipeline security partners collaboratively through the GCC/SCC/CIPAC framework.

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

With a view toward this end-state, the TSSP and this Pipeline Modal Annex specifically focus on how the Transportation Sector will continue to enhance the security of its critical infrastructure and key resources. Programs to protect the Nation's Pipeline System(s) are key to making the nation safer, more secure, and more resilient in the face of terrorist attacks and other hazards.

2 Pipeline Overview

2.1 Vision

The Pipeline Modal Annex was developed to ensure the security and resiliency of the pipeline sector. The vision of this plan is to ensure that the pipeline sector is secure, resilient, and able to quickly detect physical and cyber intrusion or attack, 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.

2.2 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 potentially can 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 based on a collaborative effort between the Federal Government and industry associations.

2.2.1 Types of Pipelines

The following are the main types of pipelines:[1]

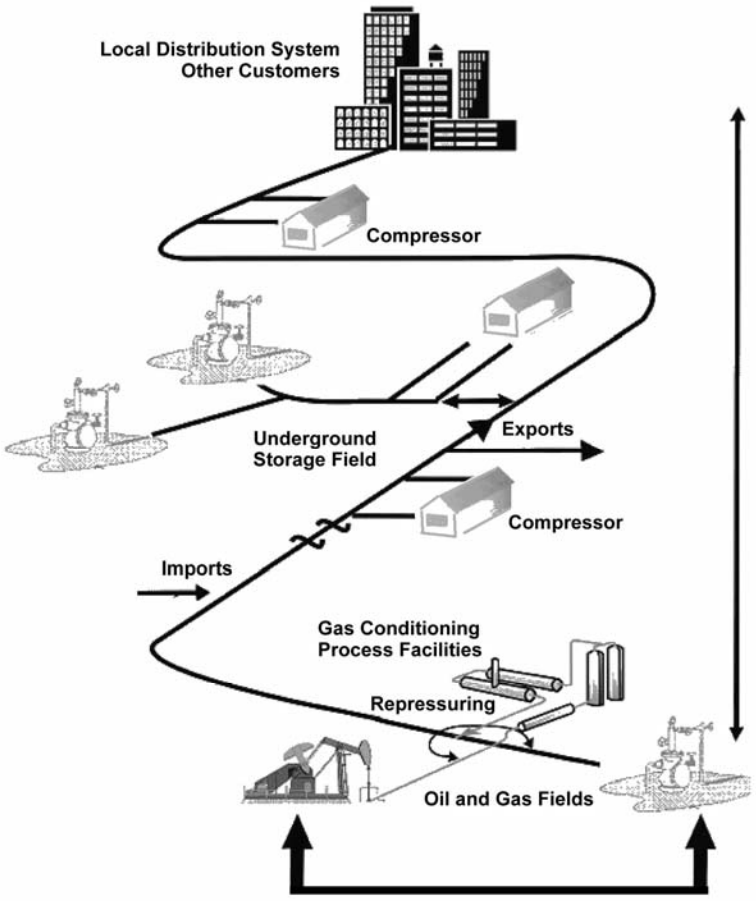
1. **Natural Gas Transmission and Storage. These lines are mostly interstate, transporting natural gas over 310,000 miles of pipelines from sources to communities, operated by more than 700 operators. More than 400 natural gas storage facilities are in the United States.**
2. **Hazardous Liquid Pipelines 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 160,000 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 operated approximately 1.9 million miles of natural gas distribution pipelines nationwide.**
4. **Liquefied Natural Gas (LNG) Processing and Storage Facilities. More than 104 facilities nationwide either directly receive LNG from tank ship or truck or receive**

[1] 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; Interstate Natural Gas Association of America

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.

Figure 1 shows the structure of a typical natural gas pipeline system.

Figure 1 Natural Gas Pipeline System



2.2.2 Threats to Pipelines

Oil and gas pipelines have been a favored target of terrorists outside the United States. While there is no specific credible reporting to date indicating that similar attacks will occur in the United States, the fact that terrorist groups have demonstrated the capability and intent to attack pipeline systems abroad raises the possibility that similar attacks could occur inside the homeland.

2.3 Government Coordinating Council (GCC) and Sector Coordinating Council (SCC) Structure and Process

A Pipeline Working Group has been established to address pipeline issues within the Energy Sector Government Coordination Council (GCC). Each of the transportation modes is required to have a 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 Sector GCC.

The Oil and Natural Gas (ONG) Sector Coordinating Council (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 SCC.

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

2.4 Federal Agencies Responsible for Pipelines

Under the NIPP, the TSA is assigned as a Sector-Specific Agency (SSA) for the Transportation Sector, including the pipeline systems mode. The U.S. Coast Guard is the SSA for the Transportation 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. DOT is responsible for administering a national program of safety in natural gas and hazardous liquid pipeline transportation, and TSA and DOT coordinate on matters relating to transportation security and transportation infrastructure protection. The Department of Justice (DOJ) through the FBI is responsible for investigating and prosecuting actual or attempted attacks on, sabotage of, or disruptions of CI/KR in collaboration with DHS.

2.5 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.

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, TSA 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 Sector. These conference calls also provide pipeline security partners with the opportunity to ask questions and bring up other important issues for discussion. Unscheduled 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: API, AOPL, INGAA, AGA, and APGA. These associations can quickly pass information to their member companies, as demonstrated by the numerous conference call information sharing sessions conducted with their respective security committees over the past 5 years.

Homeland Security Information Network (HSIN)
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 antiterrorism and incident management activities. In May 2006, the ONG SCC signed a Memorandum of Understanding (MOU) with DHS to establish the ONG HSIN. Efforts are underway to incorporate pipeline security communications and information

sharing activities into the existing HSIN system. Once completed, the pipeline mode will use the ONG HSIN.

Federal Energy Regulatory Commission (FERC) Pipeline Engineering Data and Damage Reporting

The FERC has taken steps to provide relevant engineering data that it receives from jurisdictional interstate pipelines in the context of location 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.

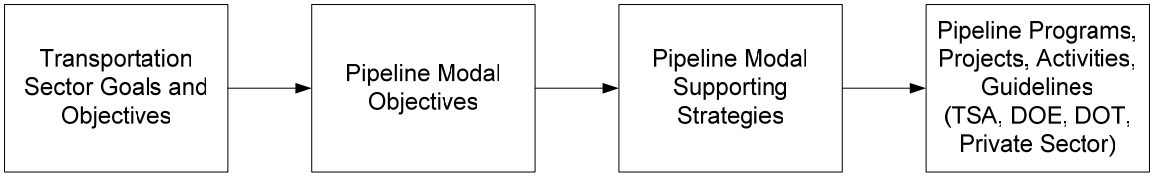
3 Implementation Plan

3.1 Goals, Objectives, and Programs/Projects/Activities

Three overarching Transportation Sector security goals and ten supporting objectives reflect the goals stated in the NIPP. The Pipeline Modal Annex outlines three objectives that aim to achieve the Transportation 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 combined contributions of TSA, other Federal, State, local, and private-sector security partners and reflect the significant efforts of all pipeline stakeholders to secure our Nation's pipeline systems.

Figure 2 shows the relationship 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 2: 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. Please refer to appendix 1 for 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 Sector Goals and Supporting Objectives

The following are the Transportation Sector overarching goals and their supporting objectives.

1. **Prevent and deter acts of terrorism using or against the transportation system**
   Supporting sector objectives

   1A. Implement flexible, layered, and effective security programs using risk management principles
   1B. Increase vigilance of travelers and transportation workers
   1C. Enhance information- and intelligence-sharing among transportation sector security partners

2. **Enhance resiliency of the U.S. transportation system**
   Supporting sector objectives

   2A. Manage and reduce the risk associated with key nodes, links, and flows within critical transportation systems to improve overall network survivability
   2B. Ensure the capacity for rapid and flexible response and recovery to all-hazards events

3. **Improve the cost-effective use of resources for transportation security**
   Supporting sector objectives

   3A. Align sector resources with the highest priority transportation security risks using both risk and economic analysis as a decision criteria
   3B. Ensure robust sector participation as a partner in developing and implementing public-sector programs for Critical Infrastructure/Key Resource (CI/KR) protection
   3C. Improve the coordination and risk-based prioritization of transportation sector security research, development, test and evaluation (RDT&E)
   3D. Align risk analysis methodologies with Risk Analysis and Management for Critical Asset Protection (RAMCAP) criteria outlined in the NIPP

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 CI/KR vulnerabilities against threats and natural perils.
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 perils.
3. **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.

These three modal objectives, which emanate from the NIPP, directly support the Transportation Sector goals and are aligned with the applicable pipeline portions of the Energy Sector goals as stated in the Energy Sector Specific Plan.

While no specific objective is directed at achieving “cost effective use of resources” stated in three sector goals, 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 benefit analysis and maximize 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 CI/KR, 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 planning 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 CI/KR 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 of 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 role/responsibility defining among 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.

3.1.4 Pipeline Programs, Projects, and Activities

The tables in sections 3.1.4.1, 3.1.4.2, and 3.1.4.3 present the programs, projects, and activities (either already undertaken or planned) that promote prevention, deterrence, preparedness, system resiliency, and information-for physical, cyber, and human 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, the pipeline modal strategies each support, and describe the security facets (e.g., cyber-security, physical infrastructure security).

3.1.4.1 TSA-Led Programs, Projects and Activities

TSA Pipeline Security 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 Corporate Security Review (CSR) programs. These two programs are briefly described in this section, but greater details are found in section 4.

Program/Project/Activity	Description	Participants	Strategies Supported	Facets
Pipeline System Relative Risk Ranking and Prioritization Tool	Statistical data used to perform relative risk ranking and prioritize CSR findings	TSA, Industry	2, 7	C, H, P
Pipeline CSR Program	On-site security reviews of pipeline company security	TSA, Industry	1, 6	C, H, P, I, N
Cyber Attack Awareness	Training and presentations on Supervisory Control and Data Acquisition (SCADA) vulnerabilities	TSA, GTI	1,3,5,7	C, I
Landscape Depiction and Analysis Tool	Incorporates combined graphic and written descriptive depiction of the pipeline domain, with risk analysis components	TSA	2, 7	C, H, P

Program/Project/Activity	Description	Participants	Strategies Supported	Facets
Pipeline Cross-Border Vulnerability Assessment Program (International)	U.S. and Canadian teams assess pipeline operations, control systems, interdependencies, and assault planning in critical cross-border infrastructure	TSA, Natural Resources Canada	1, 2, 5	I, N, P, S
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	I, N, S
Threat, Vulnerability, & Contingency Planning for Critical Pipeline Infrastructure "G8" (International)	Multinational-sharing threat assessment methodology. Advisory levels, and effective practices and vulnerability assessment information; also develops a G8-based contingency planning guidance document	TSA, DHS, Dept. of State, G8 Member Nations	6	C, H, I, N, P, S
Pipeline Policy and Planning	Coordination, development, implementation, monitoring national and TSA pipeline planning	TSA, DHS, DOT, DOE	4, 6	N, S
Regional Gas Pipeline Studies	Regional natural gas supplies studies for key markets nationwide	TSA, DOE, INGAA, GTI, NETL, Industry	2,7	D, S
Security Awareness Training Compact Discs (CD)	Informational CDs about pipeline security issues and improvised explosive devices (IED)	TSA	1, 2, 6	S
TSA Pipeline Security Stakeholder Conference Calls	Periodic information-sharing teleconference calls between TSA, government, and industry security partners	TSA, Other Government Agencies, Industry	6	N, S
Transportation 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	N, S
Pipeline Blast Mitigation Studies	Research test containing explosive tests on various configurations of pipe to determine resiliency characteristics	TSA, DOD, TSWG	1, 4, 7	D, P, R
2006 Virtual Library Pipeline Site Development	TSA Web portal for information-sharing purposes	TSA	6	S

Legend for Facets Column		
C = Cyber Infrastructure	D = Research and Development	H = Human Infrastructure
I = International	N = Network Building	P = Physical Infrastructure
R = Resiliency Enhancing	S = Information Sharing	

3.1.4.2 Other Federal Agency-Led Programs, Projects and Activities

Program/Project/Activity	Description	Participants	Strategies Supported	Facets
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	S
Homeland Security Advisory System (HSAS)	Information sharing program that makes government, the private sector and the public more vigilant when credible threat becomes available	DHS	1, 6	S
Lessons Learned Information Sharing (LLIS)	Information clearinghouse and knowledge base	DHS	3, 4, 6	S
Visualization and Modeling Working Group	Identifies risks and industry needs to improve secure control systems	DOE, DHS, Canada, Industry	4, 7	S
DOT, DOE, DHS Incident Drill Programs/Sponsorship and Participation	Tabletop and field exercises facilitation	DOT, DOE, DHS, PHMSA,	3, 4	N, R

Program/Project/Activity	Description	Participants	Strategies Supported	Facets
DOT Emergency Response and DOT-sponsored Training/Workshops	Incident response training and pipeline incident response field representatives for contingency planning, resiliency, and restore and repair capabilities	DOT, PHMSA	4, 5	R, S

3.1.4.3 Pipeline Industry-Led Programs, Projects, Activities

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

Program/Project/Activity	Description	Participants	Strategies Supported	Facets
ONG/Pipeline SCC and CIPAC Joint Sector Committee	Private-sector companies participate in the SCC and the CIPAC to engage with industry and government security partners in critical infrastructure protection discussions and activities.	Industry, Government Agencies	6	N, S
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	N, R
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	N, S
API/NPRA Security Vulnerability Assessment for the Petroleum & Petrochemical Industries	Provides practical knowledge for performing security vulnerability assessments in multiple petroleum- and petrochemical-related industries	API, NPRA	2	C, H, P, S
API Security Committee and AGA Security Committee-Sponsored Training and Workshops	Workshops/forums and training for gas and liquid petroleum industry	API	5, 6	S
Pipeline Company Security Protective and Deterrence Measures	Pipeline operators have been enhancing protective and deterrence measures in accordance with Pipeline Security Circular 2002	Pipeline Companies	1	C, H, P

3.2 Pipeline Security Smart Practices, Security Guidelines, Security Standards, and Compliance and Assessment Programs

Various smart practice documents, guidelines, and standards have been developed and implemented within the pipeline mode that supports the modal objectives. These efforts are described in the tables below.

3.2.1 TSA Smart Practices, Guidelines, Standards, and Programs

Practices/Guidelines/Standards/ Program	Description	Participants	Strategies Supported	Facets
Pipeline Security Smart Practices	Document to assist hazardous liquid and natural gas pipeline industries in their security planning and implementation	TSA, Industry	1, 4	C, H, P, S
DOT Pipeline Security Guidelines, 2002	Guidelines that suggest minimum security levels for prevention, deterrence, and security incident response	TSA, DOT	1, 6	C, H, P, S

3.2.2 Industry Smart Practices, Guidelines, Standards, and Programs

Practices/Guidelines/Standards/Program	Description	Participants	Strategies Supported	Facets
Security Guidelines; Natural Gas Industry, Transmission and Distribution: Assessment Guidelines	Provide an approach for vulnerability assessment, critical facility definition, detection/deterrent methods, response and recovery, cyber-security, and relevant operational standards	AGA, INGAA, and APGA	1	C, H, P, S
Cryptographic Protection of Supervisory Control and Data Acquisition (SCADA) Communications	Define encryption methods for SCADA systems	AGA	1	C, R
API Security in the Petroleum Industry: Practices Guidelines	Recommend security practices for all segments of liquid and gas petroleum	API	2	C, H, P
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	C, S
API Information Management and Technology Program	Provide a comprehensive review and quantitative assessment of company security programs	API	2	C, S

3.3 Federal Grant Programs

The following Federal grant program supports the Pipeline Modal objectives and strategies.

Program/Project/Activity	Description	Participants	Strategies Supported	Facets
Buffer Zone Protection Program	Provide resources to identify and mitigate vulnerabilities of critical infrastructure	Federal, State, local governments; Industry	1, 7	P, R

3.4 Way Forward

TSA will continue to participate in all aforementioned programs, projects, and activities. However, the core of TSA's efforts is the CSR process and the Pipeline System Relative Risk Assessment and Prioritization methodology, which will continue to grow year by year. These efforts are described in greater detail in section 4.

In addition, TSA plans to address needed improvements and gaps in the following areas to improve security awareness.

International
The relationship with Canada has proven to be extremely worthwhile and the plan is to establish a working relationship and program within fiscal years 2007 and 2008.

National
Although progress has been made establishing roles and responsibilities with government and industry partners, further definition and programs must be established. The sector partners need to expand to other industry, regional, State, and tribal governments. These programs need to be established in fiscal years 2007, 2008, and 2009.

Training and Exercises
Industry partners have established security training programs and TSA produced a training CD in 2006. However, there are no training standards established, and many aspects of the sector are not involved in any training programs. These programs are under development and will be expanded in each fiscal year as appropriate.

4 Risk-Based Approach to Pipeline Security

This section is included to provide detail on how TSA will use risk-based programs to achieve the overarching Transportation Sector goals. It should be noted that it deviates from the model the other modal implementation plans followed. "Program Management" is found instead in section 5.

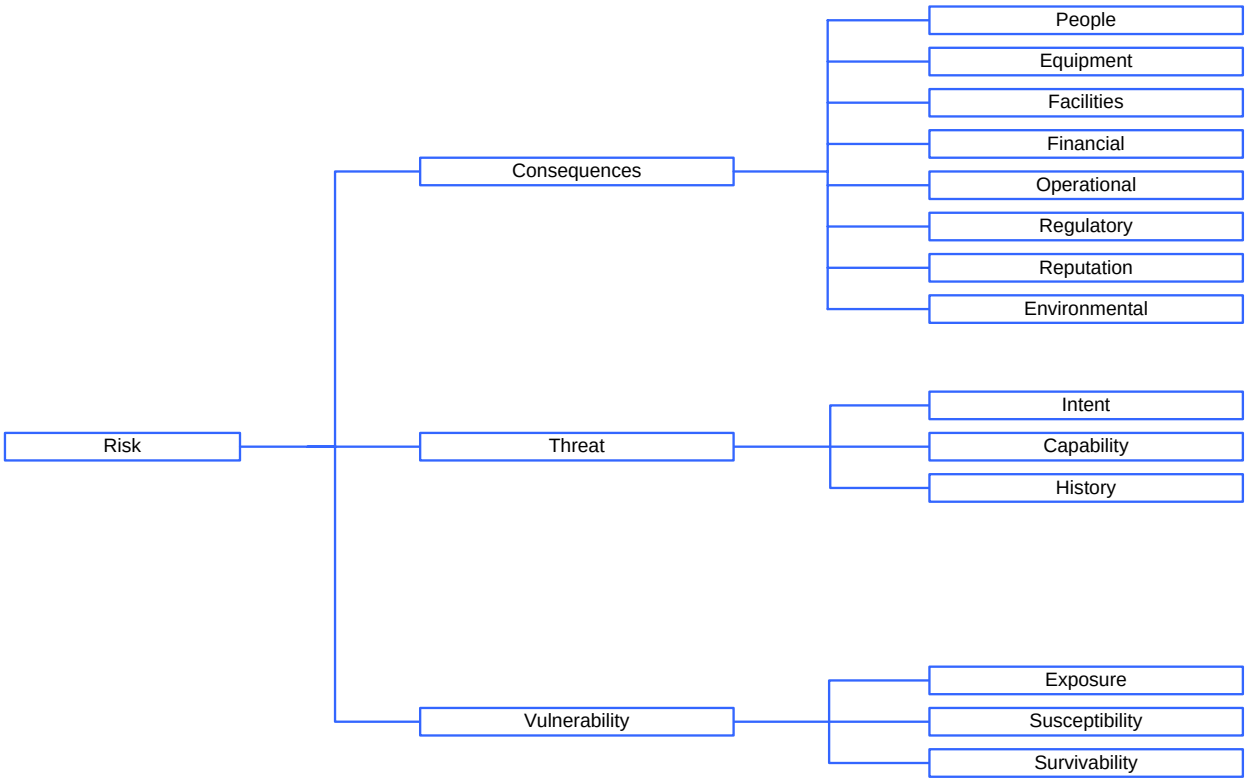
4.1 Defining and Measuring Risk

In practical terms, a risk-based approach to security is recognizing that there are too many risk scenarios to protect all risks equally, so we have to establish priorities and allocate security resources accordingly. A more theoretical description of risk is that it is a function of likelihood (mathematically expressed as a probability) multiplied by the consequences (in terms of people, facilities, financial loss, operational disruption, etc.). Likelihood can be further broken down into threat (an adversary's capability + 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. We try to measure the various parts of risk for which information is available and make some judgment calls where it is not.

Figure 3 shows the framework that will be used to define risk for the purposes of this approach.

Figure 3: Risk Definition Framework



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

TSA Pipeline Security relies on TSA's Office of Intelligence to provide threat assessments based on information received from the Intelligence Community: the Federal Bureau of Investigation (FBI), Central Intelligence Agency (CIA), DHS Office of Intelligence and Analysis, and others. When there is specific threat information about a pipeline facility or system, TSA Pipeline Security will enlist the aid of TSA's Office of Law Enforcement to conduct a joint vulnerability assessment of the targeted facility and provide the report, with options for consideration, to the pipeline operator. These joint vulnerability assessments (JVA) are done in concert with representatives from other parts of DHS as well as the local Joint Terrorism Task Force.

4.2 Pipeline System Relative Risk Assessment and Prioritization

The natural gas and hazardous liquids pipeline system infrastructure is a large, widely dispersed, and mostly privately-owned system. While there is a desire to secure all aspects of all critical infrastructures, the total pipeline system universe 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 Assessment and Prioritization methodology that provides a logical prioritization process is required to list systematically, analyze, and sort pipeline systems and critical pipeline components within those pipeline systems. TSA will do the prioritization exclusively with input from pipeline operators and industry trade associations. By prioritization, government security resources can be used effectively to manage risk mitigation to protect critical pipelines from terrorist threats. Pipeline systems will always be ranked and evaluated first before any specific asset or component. The overall guidance for the methodology is introduced in section 3.2 of the Transportation Sector Specific Plan.

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

4.3 Pipeline Relative Risk Ranking

In the case of the pipeline industry, the over arching objective is to protect crucial energy supply to commercial, industrial, and domestic users. The process requires a strong understanding of the pipeline industry. The objective is to focus attention on the pipeline systems that, if damaged, could have the greatest impact to energy supplies and national security.

In the first step, TSA 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 criticality of certain systems quantitative methods do not adequately address.

4.4 System Screen and Asset Identification

TSA will continue to gather data by conducting CSR 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 will be 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 above ground piping**
- **Storage facilities**

In addition to the above, TSA is sponsoring regional gas studies of key markets in the United States in cooperation with DOE. These studies, which have been ongoing since 2003, improve our understanding of which regions are most vulnerable to gas supply disruptions, and they provide a sense of what the consequences of those disruptions might be. TSA will continue to evaluate pipeline networks comprised of separate pipeline systems or companies serving a region (the northeast U.S., the West coast, etc.). Regional criticality can vary depending on seasonal usage, weather, or other factors but will be evaluated based on worst-case scenarios. TSA also examines high-level dependencies and interdependencies with other regions and systems. Pipelines serving regions with critical needs and greater vulnerability will be ranked higher in the screening process.

4.5 Detailed System and Asset Assessment (Future State)

TSA plans to conduct more detailed System and Asset Assessment programs. Private pipeline sector 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, system 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 resiliency 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 cyber-security 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 federally 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 in current use and each varies in assessment approach. RAMCAP, Site Assistance Visits (SAV), and TSA's JVAs are examples of field assessment tools. As outlined in the DHS NIPP, flexibility on the approaches taken is given as long as it conforms to the basic criteria outlined in the NIPP.

Assessment teams will perform on-site facility security evaluation of several items including:

- **Access control**
- **Closed circuit TV and intrusion detection systems**
- **Barriers and fencing**
- **Power supply and backup generators**
- **Telecommunications and other interdependencies**
- **On-site security personnel**
- **Local law enforcement and emergency response resources**

4.6 Prioritization

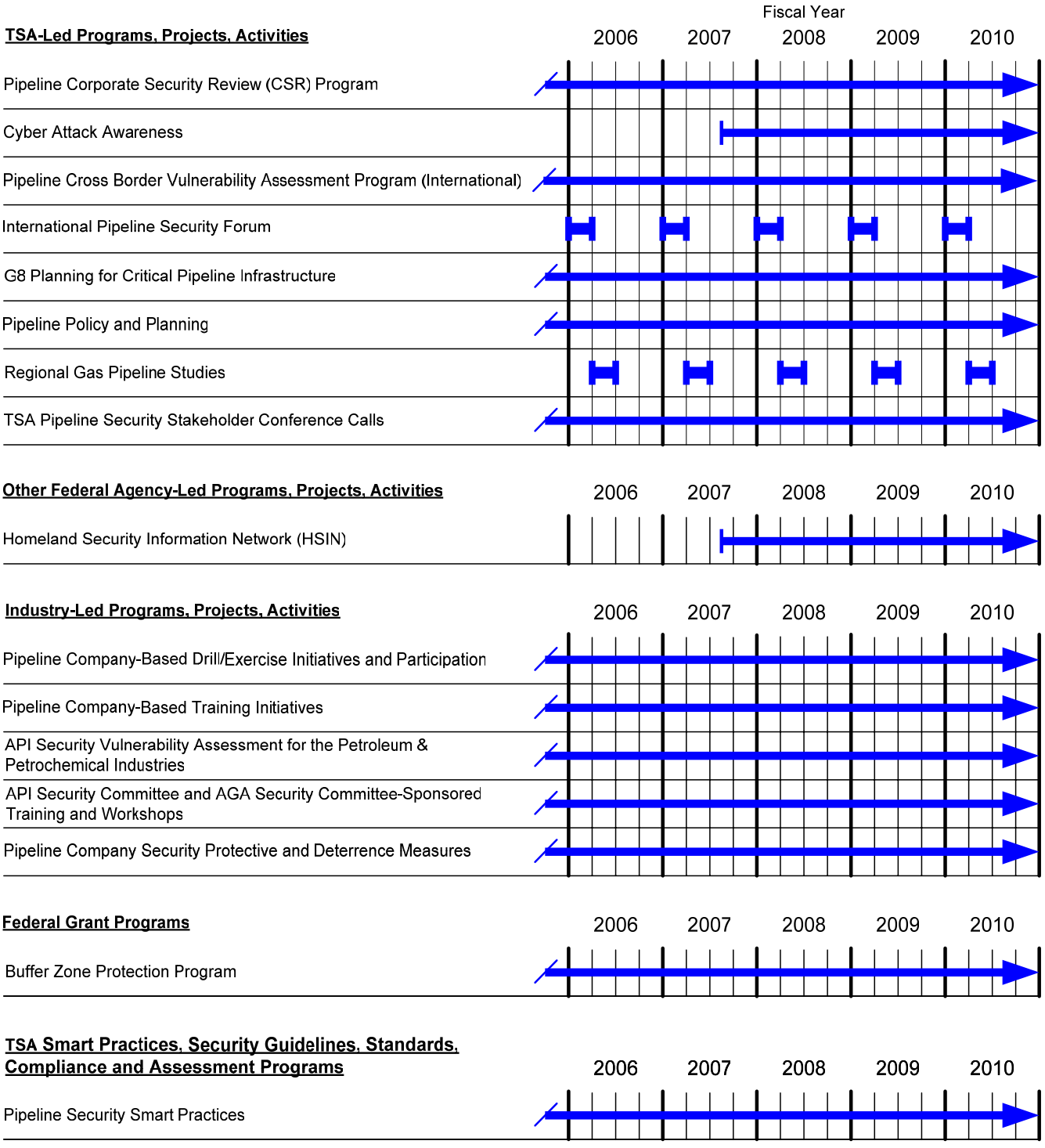
TSA will use a pipeline system relative risk assessment and prioritization methodology to rank the most critical systems and assets according to the greatest importance to energy supplies and risk, in threat, vulnerability, and consequences. The list will be sorted using proven qualitative and quantitative 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. In the future, within each assessed pipeline system, individual component assets will be also ranked in the same manner. With periodic reevaluation, the ranking list will probably change over time. In addition, subject matter experts will use their knowledge to verify the algorithm's results.

5 Pipeline Security Program Management

TSA uses the GCC/SCC/CIPAC framework to develop and coordinate program activities. To enable participation of government and industry stakeholders, TSA conducts monthly conference calls, visits pipeline operators periodically to conduct corporate security reviews, and participates in the GCC and CIPAC meetings. TSA and the DOT's Pipeline and Hazardous Materials Safety Administration (PHMSA) have jointly developed a pipeline annex to the DOT/DHS MOU to further clarify their roles in pipeline security and safety, respectively.

The following charts show the implementation timelines for the program activities that are designed to identify and address gaps in pipeline security.


Fiscal Year
TSA-Led Programs, Projects, Activities
2006
2007
2008
2009
2010
Pipeline Corporate Security Review (CSR) Program
Cyber Attack Awareness
Pipeline Cross Border Vulnerability Assessment Program (International)
International Pipeline Security Forum
G8 Planning for Critical Pipeline Infrastructure
Pipeline Policy and Planning
Regional Gas Pipeline Studies
TSA Pipeline Security Stakeholder Conference Calls
Other Federal Agency-Led Programs, Projects, Activities
Homeland Security Information Network (HSIN)
Industry-Led Programs, Projects, Activities
Pipeline Company-Based Drill/Exercise Initiatives and Participation
Pipeline Company-Based Training Initiatives
API Security Vulnerability Assessment for the Petroleum & Petrochemical Industries
API Security Committee and AGA Security Committee-Sponsored Training and Workshops
Pipeline Company Security Protective and Deterrence Measures
Federal Grant Programs
Buffer Zone Protection Program
TSA Smart Practices, Security Guidelines, Standards, Compliance and Assessment Programs
Pipeline Security Smart Practices

6 Security Gaps

The following is a list of security gaps that are currently being addressed in each of the programs listed in Section 3.1.4 of this Annex.

1. The TSA pipeline security division conducts Corporate Security Reviews to assess pipeline security. The intent of these onsite security reviews of pipeline companies is to develop first hand knowledge of security planning and execution at critical pipeline systems, establish communication with key pipeline security personnel, and identify and share smart practices. As industry wide security gaps are identified through the CSR process, the TSA pipeline security division develops programs to address gaps throughout the pipeline industry.

2. Cross border (International) pipelines are becoming increasingly important to the nations 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. Four pipeline systems have been reviewed by a joint U.S./Canadian team, the most recent in June 2006. It is planned to conduct an additional system assessment this year.

3. While the security of individual pipeline systems has been addressed, regional studies evaluating potential service disruptions have not been conducted. To address this problem, regional gas studies are being conducted. These projects assess the capabilities and resiliencies of the nation's natural gas delivery infrastructure to withstand service disruption, and examine the range of implications in the event of any natural gas disruption. The studies, conducted by contractor staff, develop information and analyses to allow Federal and state agencies and other interests to develop effective security policies and restoration plans to assure natural gas deliveries in the face of potential disruptions. TSA is a member of the Steering Council for this project.

4. 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 a training CD. 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 worked with industry partners to develop the training compact disc (CD) for distribution to pipeline stakeholders.

5. Due to the industry dependence on remote control systems, cyber threats continue to be an area of concern. The TSA has two programs and objectives addressing this gap. First, Supervisory Control and Data Acquisition (SCADA) systems are used by the pipeline industry to monitor and remotely control their pipelines. It is technically possible for hackers, terrorists, or foreign governments to access these SCADA systems to obtain confidential information and/or to damage the systems using the remote control. TSA partnered with Gas Technologies Institute to develop presentation material to illustrate existing SCADA vulnerabilities and consequently increase the cyber security awareness of pipeline companies. Second, Supervisory Control and Data Acquisition (SCADA) systems are increasingly important to the operation of the nation's pipelines. A program of SCADA security evaluation is a necessary addition to TSA Corporate Security Reviews (CSR) in order to assess the vulnerability of these networks to cyber attack. This program is intended to become an adjunct to the CSR program. It will continue in an ongoing basis.

6. To ensure continued domain awareness and information sharing, the TSA pipeline security division conducts an annual pipeline international forum, monthly conference calls, provides suspicious incident reports to the industry, actively participates in the industry GCC and SCC, and plans to revise the pipeline security guidelines.

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

Pipeline Modal Objectives	Supporting Strategies	Supporting Programs, Projects, Activities, Guidelines, etc.	TSSP Objectives Supported
1. Reduce level of risk through analysis and implementation of security programs that enhance deterrence and mitigate CI/KR vulnerabilities against threats and natural perils.	1) Implement layered threat deterrence and vulnerability mitigation programs.	Cyber Attack Awareness Pipeline Cross Border Vulnerability Assessment Program Pipeline Corporate Security Review (CSR) Program Security Awareness Training CD Pipeline Security Smart Practices Pipeline Blast Mitigation Studies	1A. Implement flexible, layered, and effective security programs using risk. 2A. Manage and reduce the risk associated with key nodes, links, and flows within critical transportation systems to improve overall network survivability. 3A. Align sector resources with the highest priority transportation security risks using both risk and economic analysis as a decision criteria. 3B. Ensure robust sector participation as a partner in the development and implementation of public sector programs for CI/KR protection. 3D. Align risk analysis methodologies with Risk Analysis and Management for Critical Asset Protection (RAMCAP) criteria outlined in the NIPP.
	2) Develop and perform collaborative risk analysis processes.	Landscape Depiction and Analysis Tool Pipeline Cross-Border Vulnerability Assessment Program Regional Gas Pipeline Studies Pipeline System Relative Risk Ranking and Prioritization 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 perils.	3) Use collaborative plan development and drill/exercise participation.	Pipeline Security Regulations 193.2900, 193.2905/NFPA 59A DOT Sponsored exercises Company Based Drill/Exercises Participation Lessons Learned Information Sharing (LLIS)	2A. Manage and reduce the risk associated with key nodes, links, and flows within critical transportation systems to improve overall network survivability. 2B. Ensure the capacity for rapid and flexible response and recovery to all-hazards events, 3A. Align sector resources with the highest priority transportation security risks using both risk and economic analysis as a decision criteria. 3B. Ensure robust sector participation as a partner in developing and implementing of public sector programs for CI/KR protection.
	4) Promote pipeline system resiliency and contingency capability enhancement measures.	Threat, Vulnerability, & Contingency Planning for Critical Pipeline Infrastructure “G8” Pipeline Policy and Planning Pipeline Blast Mitigation Studies	
	5) Conduct security-related training that enhances domain awareness.	DOT-sponsored Contingency, Resiliency, Response, Restore training/workshops	

Pipeline Modal Objectives	Supporting Strategies	Supporting Programs, Projects, Activities, Guidelines, etc.	TSSP Objectives Supported
3. Increase the level of domain awareness, information-sharing and response planning and coordination through enhanced training, network building and efficient research, development application.	5) Conduct security-related training that enhances domain awareness.	DOT-sponsored Contingency, Resiliency, Response, Restore training/workshops Security Awareness Training CD API/AGA Workshops	1B. Increase vigilance of travelers and transportation workers 1C. Enhance information and intelligence sharing among transportation sector security partners. 3A. Align sector resources with the highest priority transportation security risks using both risk and economic analysis as a decision criteria. 3B. Ensure robust sector participation as a partner in the developing and implementing public sector programs for Critical Infrastructure/Key Resources (CI/KR) protection. 3C. Improve the coordination and risk-based prioritization of transportation sector security Research, Development, Test and Evaluation (RDT&E).
	6) Conduct network enhancement and information-sharing activities.	Cyber Attack Awareness Pipeline Cross Border Vulnerability Assessment Program CSR Program International Pipeline Security Forum Threat, Vulnerability, & Contingency Planning for Critical Pipeline Infrastructure G8 Pipeline Policy and Planning Security Awareness Training CDs Pipeline Security Smart Practices TSA Pipeline Security Stakeholder Conference Calls Virtual Library Pipeline Site Development Pipeline Company-Based Security Training Initiatives	
	7) Conduct research and development and other activities that build domain awareness.	Cyber Attack Awareness Landscape Depiction and Analysis Tool Regional Gas Pipeline Studies, Pipeline System Relative Risk Ranking and Prioritization Tool Pipeline Blast Mitigation Studies	

Appendix 2. Descriptions of Programs, Projects, Activities, Guidelines, and Standards

TSA-Led Programs, Projects, and Activities

Pipeline System Relative Risk Ranking and Prioritization Tool

This program and associated activities are currently being developed within TSA. It compiles statistical data on pipeline systems that will be used to perform a relative risk ranking and to prioritize CSR results/findings to maximize focus and direction of resources toward these areas. This program supports strategies 2 and 7.

Pipeline CSR Program

Since 2003, TSA has been conducting CSRs, and on-site security reviews, 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. This program supports strategies 1 and 6.

Cyber Attack Awareness

TSA is partnering with Gas Technology Institute (GTI) to develop training and presentation material to illustrate existing supervisory control and data acquisitions (SCADA) vulnerabilities and consequently increase the cyber-security awareness of pipeline companies. This program supports strategies 1, 3, 5, 7.

Landscape Depiction and Analysis Tool

Currently under development, this tool incorporates a combined graphic and written descriptive depiction of the pipeline domain. It is also both a risk analysis tool that can be used in analysis of threats, vulnerabilities, and consequences (TVC) as they are related to specific types of pipeline facilities within a system. This program supports strategies 2 and 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. This program supports strategies 1, 2, and 5.

International Pipeline Security Forum

TSA, in conjunction with Natural Resources Canada, annually hosts the International Pipeline Security Forum. This international forum provides an opportunity for U.S. and Canadian governments and industry pipeline officials to discuss security issues and topics. This program supports strategies 5 and 6.

Threat, Vulnerability, and Contingency Planning for Critical Pipeline Infrastructure "G8" (International)

This three-piece project includes forming consensus on determining threat methodologies for critical pipeline infrastructure, forming consensus on effective practices associated with conducting vulnerability assessments of pipelines and critical

nodes/facilities, and developing a G8-based contingency planning guidance document that provides practices and approaches used to protect /secure critical pipeline infrastructure against the threat of terrorism. TSA is working closely with both the Department of State and the DHS headquarters to develop a contingency guidance document that provides smart practices and approaches for protecting and securing critical pipeline infrastructure against terrorist threats. Member states may use this information to prepare and implement effective security measures and better respond to specific threat conditions. This program supports strategy 6.

Pipeline Policy and Planning

TSA, in collaboration with other Federal and private industry security partners, coordinates, develops, implements, and monitors National and TSA-specific plans such as TSSP, Performance Assessment and Rating Tool (PART), National Asset Database (NADB) and Continuity of Operations Plans (COOP). TSA participates on DHS planning activities such as the TSA strategic, acquisition and business planning activities, and monitors performance of the same. Additionally, TSA implements and manages planning, metrics, and milestones and coordinates with the other transportation modes as well as other DHS and interagency threat and risk-based planning efforts such as the Strategic Homeland Infrastructure Risk Assessment (SHIRA) and event-driven risk analysis. This program supports strategies 4 and 6.

Regional Gas Pipeline Studies

TSA, in cooperation with the Department of Energy (DOE), is sponsoring a study of regional natural gas supplies for key markets nationwide. These studies, which have been ongoing since 2003, use computer-based modeling to evaluate the impact of a major pipeline disruption as the result of a terrorist attack. As of 2006, most regions of the country have been evaluated. The prime contractor for the effort is the National Energy Technology Laboratory, and the GTI does the technical analysis, with support from Science Applications International Corporation (SAIC). This program supports strategies 2 and 7.

Security Awareness Training Compact Discs (CD)

TSA developed two compact discs (CD) for distribution to pipeline transmission and distribution companies. The general focus of the CD is toward stakeholders and their employees who have the need for a basic level of awareness and understanding of pipeline security. A more in-depth security awareness CD was also developed for those whose responsibilities include or greatly affect pipeline security, such as security personnel. This CD focuses on more in-depth analysis of terrorist mindset and characteristics and improved identification of improvised explosive devices (IED) and vehicular borne improvised explosive devices (VBIED). In addition, this CD contains other informational "tools" that would be of assistance to the pipeline security. This program supports strategies 1, 2 and 6.

TSA Pipeline Security Stakeholder Conference Calls

See section 0 for information on these regularly scheduled calls. This program supports strategy 6.

2006 Virtual Library Pipeline Site Development

Currently under development within TSA, this project and its related activities will create a TSA Pipeline Security informative Web site on the TSA Virtual Library for information-

sharing among pipeline modal stakeholders and other transportation mode personnel within TSA. This program supports strategy 6.

Pipeline Blast Mitigation Studies

This is a research test project involving the multi-agency Technical Support Working Group (TSWG), DOD, and TSA. The project entails conducting explosive tests on various configurations of pipe to determine resiliency characteristics. This program supports strategies 1, 4, and 7.

Other Federal Agency-Led Programs, Projects and Activities

Homeland Security Information Network (HSIN)

HSIN is an information-sharing tool DHS Infrastructure Protection Office developed in partnership with the private sector that provides a secure/nonsecure Web-based source for security-related information, threat intelligence, and indications and warnings. This program supports strategy 6.

Homeland Security Advisory System (HSAS)

HSAS is an information-sharing program that improves security by making government, the private sector, and the public more vigilant when credible threat information of terrorist activity or intentions becomes available. DHS is responsible for system operation, to include intelligence assessment, setting appropriate HSAS level, educating users about the system, and disseminating advisories through multiple media. This program supports strategies 1 and 6.

Lessons Learned Information Sharing (LLIS)

DHS facilitates the LLIS program, which entails an information clearinghouse and knowledge base that promotes dissemination of vetted, static-type reference information, standards, guidelines, lessons learned, and best practices to the transportation stakeholder community while maintaining adherence to consistent, systematic DHS vetting criteria. By promoting awareness of threats and transportation security vulnerabilities, LLIS will enable an agile incident-response capability for stakeholders through promoting programs, processes, and activities that enhance security. This program supports strategies 3, 4 and 6.

Visualization and Modeling Working Group

The Visualization and Modeling Working Group is a joint program between DOE, DHS, Public Safety Emergency Preparedness Canada, Natural Resources Canada, and the private sector that identifies risks and industry needs to improve secure control systems. This program supports strategies 4 and 7.

DOT Incident Drill Programs/Sponsorship and Participation

The Department of Transportation Pipeline and Hazardous Materials Safety Administration Office of Pipeline Safety (OPS) leads table top and field exercises with Federal, State, local, and tribal environmental protection, law enforcement, emergency management, public, media, and energy industry representatives. PHMSA OPS helps design, conduct, and evaluate exercises with government, public, and industry partners. This program supports strategy 3.

DOT Emergency Response and DOT-sponsored Training/Workshops on Contingency Planning, Resiliency, Emergency Response, and Restore and Repair Capabilities

PHMSA serves on the National Coordinating Committee with the United States Coast Guard, Minerals Management Service, and the Environmental Protection Administration. The Committee seeks to better protect people and the environment from oil spills. PHMSA trains representatives in the National Incident Management System, Unified Command, Emergency Communication, and hazardous waste operations and emergency response (HAZWOPER). PHMSA representatives work in the field and in the Crisis Management Center to respond to natural and human made disasters that may involve pipelines. This program supports strategies 4 and 5.

Pipeline Industry-Led Programs, Projects, Activities

Pipeline Company-Based Security Training Initiatives

Security awareness and training are elements included in the Federal Government and industry guidelines. Initiatives include corporate and field training and usually include response measures tied to the DHS Homeland Security Advisory System. Tools include briefings, manuals, CDs, and computer-based training. This program supports strategy 5.

Pipeline Company-Based Drill/Exercises Initiatives

Since 2002, both at the regional and national level, pipeline operators have been participating in drills/exercises related to infrastructure security at all levels (Federal, State, regional, local, and corporate). Since energy is a critical infrastructure and key player in interdependencies with other sectors of the economy, pipelines have engaged in tabletop and on-site simulated exercises. These include terrorist and natural disaster scenarios. Since most operators are regulated at the State level, this includes drills/exercises by state commissioners and governors direct. This program supports strategy 3.

API/NPRA Security Vulnerability Assessment for the Petroleum & Petrochemical Industries

This informative and instructional guide provides practical hands-on knowledge for performing security vulnerability assessments in multiple petroleum and petrochemical-related industries. This program supports strategy 2.

API Security Committee and AGA Security Committee-Sponsored Training and Workshops

Each association's related security committees hold workshops/forums and training for gas and liquid petroleum industry to discuss/share information and educate members on security-related issues. This program supports strategies 5 and 6.

Pipeline Company Security Protective and Deterrence Measures

Since the issuance of and in accordance with the Pipeline Security Circular 2002 and the industry-developed guidelines, pipeline operators have been enhancing protective and deterrence measures. Measures include supplementing current emergency plans with terrorist risk elements, strengthening physical barriers, tightening access controls, adjusting frequency of patrols, and confirming response and recovery actions with local law and emergency officials. This program supports strategy 1.

TSA Smart Practices, Guidelines, Standards, Compliance and Assessment Programs

Pipeline Security Smart Practices

The "Pipeline Security Smart Practices" reflect the application of data collected during the CSR process. This document is intended to assist the hazardous liquid and natural gas pipeline industries in their security planning and implementing security measures to protect their facilities, their assets, their people, and the public. This program supports strategies 1 and 4.

DOT Pipeline Security Guidelines, 2002

Initially developed within DOT in conjunction with pipeline industry partners and adopted by TSA after its creation, these guidelines suggest minimum security levels for prevention, deterrence, and security incident response. Additionally, they provide a baseline and guidance for conducting assessments and determining criticality level. This program supports strategies 1 and 6.

Industry Smart Practices, Guidelines, Standards, Compliance and Assessment Programs

AGA, Interstate Natural Gas Association of America, and American Public Gas Association, Security Guidelines: Natural Gas Industry, Transmission and Distribution: Assessment Guidelines

Based on the DOT Pipeline Security Guidelines, 2002, these guidelines were issued in September 2002 and provide an approach for vulnerability assessment, critical facility definition, detection/deterrent methods, response and recovery, cyber-security, and relevant operational standards for the natural gas industry. This program supports strategy 1.

Cryptographic Protection of Supervisory Control and Data Acquisition Communication (SCADA)

Developed primarily by AGA, these guidelines define a data encryption protocol method for securing SCADA systems against possible cyber-security attacks. This program supports strategy 1.

American Petroleum Industry (API) Security in the Petroleum Industry: Practices Guidelines

These guidelines recommend security practices for all segments of the sector involving liquid and gas petroleum energy commodities. This program supports strategy 1.

API Pipeline SCADA Security Standard (API Standard 1164)

This API-developed guideline provides a model for proactive industry actions to improve the security of the Nation's energy infrastructure. This program supports strategy 1.

API Information Management and Technology Program

This API program provides a comprehensive review and quantitative assessment of company security programs, with the focus on due care requirements, database of security programs, and compliance initiatives. This program supports strategy 2.

Federal Grant Programs

Buffer Zone Protection Grants Program

This program is a DHS-sponsored grant program designed to provide resources to State, local, and tribal law enforcement operators to facilitate vulnerability identification and mitigation discussion between security partners and individual owners and operators. This program supports strategies 1 and 7.