CHARACTERISTICS AND COMMON VULNERABILITIES INFRASTRUCTURE CATEGORY: PETROLEUM PIPELINES

Protective Security Division
Department of Homeland Security

Draft - Version 1, February 26, 2004

Preventing terrorism and reducing the nation's vulnerability to terrorist acts require understanding the common vulnerabilities of critical infrastructures, identifying site-specific vulnerabilities, understanding the types of terrorist activities that likely would be successful in exploiting those vulnerabilities, and taking preemptive and protective actions to mitigate vulnerabilities so that terrorists are no longer able to exploit them. This report characterizes and discusses the common vulnerabilities of petroleum pipelines, which are located nationwide and transport more than two-thirds of all the crude oil and refined products in the United States.

PETROLEUM PIPELINE CHARACTERISTICS

The United States (U.S.) has two types of pipelines that transport petroleum: those that carry crude oil and those that carry refined petroleum products, such as gasoline, diesel fuel, jet fuel, and home heating oil. Pipelines transport more than two-thirds of all crude oil and refined products in the U.S. Other transportation modes are water, which includes ocean tankers and barges and accounts for 28% of petroleum transportation; tanker trucks, which account for 3% of petroleum transportation; and railroads, which account for 2% of petroleum transportation. The U.S. has more than 200,000 miles of petroleum pipelines. Pipelines dominate petroleum transportation because they are safe (according to statistics compiled by the National Transportation Safety Board) and cost-effective and because they reduce traffic and pollution. Figures 1 and 2 are maps of the network of crude oil and refined product pipelines in the U.S., respectively.

The network of petroleum pipelines that serve the U.S. is not a single entity. Pipeline systems that serve large regions of the country or move petroleum from one region to another are owned and operated both by large oil companies (e.g., Shell, BP, ExxonMobil) and by companies that are only pipeline operators, that is, that are not involved in other aspects of the oil industry. In addition, companies, such as a power plant or a chemical plant, may operate a small pipeline system to bring fuel to the plant or to move feedstocks from one plant to another.

Crude oil pipelines are subdivided into trunk lines and gathering lines. Approximately 55,000 miles of trunk lines connect regional markets in the U.S. Trunk lines are usually 8 to 24 inches in diameter but can be as large as 48 inches. The Trans Alaska Pipeline System (TAPS) is the largest trunk line in the U.S. It transports oil about 800 miles from the North Slope of Alaska to the ice-free port of Valdez, Alaska. More than one-half of that pipeline is aboveground so as not to melt the permafrost in the region.

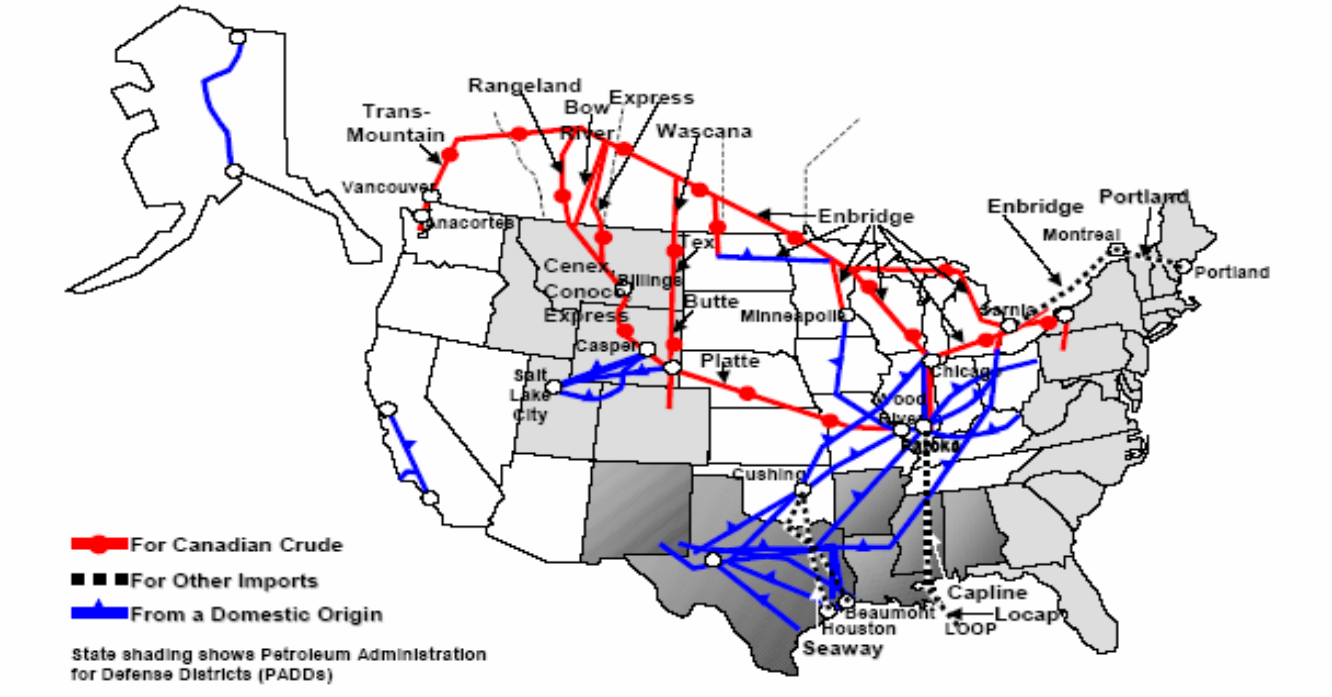


Figure 1 Crude Oil Pipeline Network

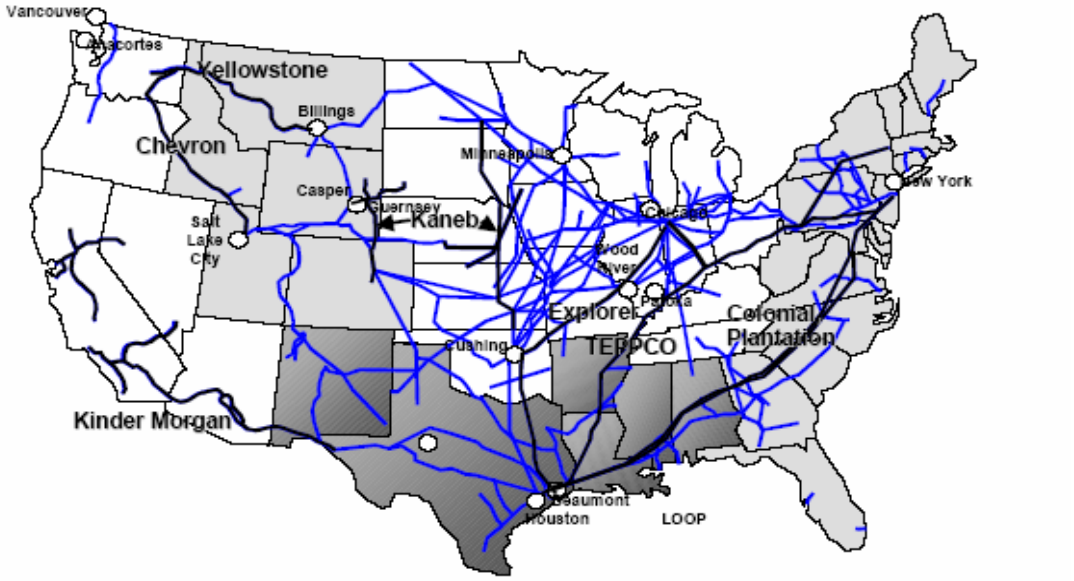


Figure 2 Refined Product Pipeline Network

Gathering lines are small lines (usually 2 to 8 inches in diameter) that collect oil from many wells and connect to trunk lines. There are approximately 30,000 to 40,000 miles of gathering lines located primarily in Texas, Oklahoma, Louisiana, and Wyoming.

Refined product pipelines transport refined product from refineries to terminals or local distribution centers. These pipelines can vary in size from as small as 8–12 inches to as large as 42 inches in diameter. Larger diameter pipes are used in trunk lines that deliver product from a refining area to a consuming region. Smaller diameter pipelines distribute the product to local areas. There are approximately 95,000 miles of refined product pipeline in the U.S.; these pipelines can be found in almost every state with the exception of some New England states as shown in Figure 2. Major U.S. airports rely almost entirely on dedicated pipelines for direct delivery of jet fuel.

Most oil pipelines are “common carriers” under the Interstate Commerce Act. They provide transportation, temporary storage, and logistics services. They do not necessarily own the product they transport. Shippers, such as refiners, marketers, and owners of oil, contract for space on an oil pipeline. As common carriers, pipelines must allocate space to all shippers who meet their conditions of service. These conditions are publicly posted and must not be unduly discriminatory.

Different grades of crude oil or various refined products are usually transported through the same pipeline in assorted batches. Batching is conducted either with or without a physical barrier separating the two products. Mixing between batches is small and can be controlled. The product mixture, called transmix, is typically diverted to tanks and either reprocessed on site or moved via truck to a reprocessing center or returned to a refinery. When no barrier exists between different products, the difference in density of the two materials maintains the separation (under pressure and in turbulent flow) with only a short length interval in which mixing occurs. The position of each batch and the extent of mixing can be monitored at points along the line by measuring the density of the fluid in the line. An inflated rubber sphere or ball can be used as a physical barrier between batches to separate them.

Oil moves through pipelines at speeds of 3 to 8 miles per hour. Pipeline transport speed depends on the diameter of the pipe, the pressure under which the oil is being transported, and other factors, such as the topography of the terrain and the viscosity of the oil being transported. At that speed, it takes about 12 days to move oil from the Gulf Coast to Chicago, a distance of about 1,000 miles.

Common Components

Common components of petroleum pipeline systems include the pipeline, pump stations, storage fields and tank farms, block valve stations, and control centers.

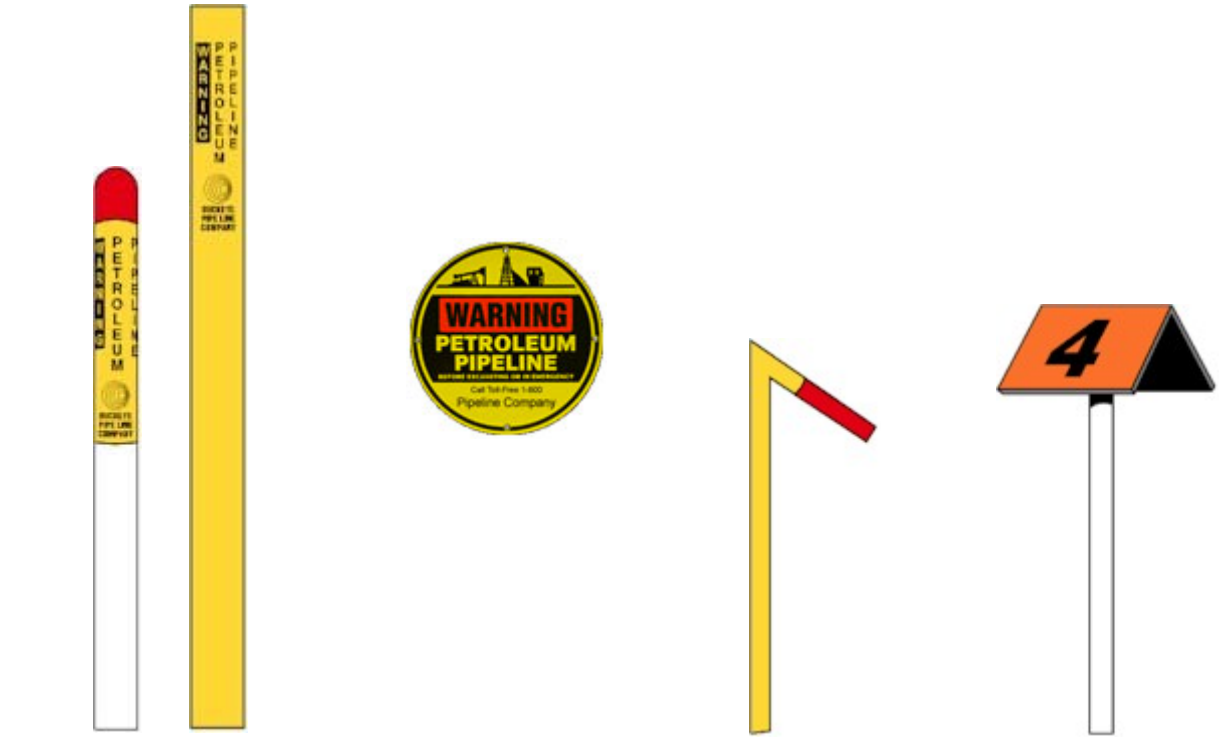
Pipeline

Steel pipe is used in pipeline construction and is commonly called line pipe to distinguish it from other types of pipe and tubing used in the oil industry. Line pipe varies in thickness, up to 0.5 inch. The pipeline is covered with a protective coating, and most pipelines are buried

underground. Burial depth may vary depending on local geologic conditions along the pipeline route.

Underground pipelines need additional corrosion protection because of differences in electric potential between the pipeline and underground materials. A cathodic protection system is used to protect nearly all underground pipelines. In this system, anodes or "ground beds" are constructed at strategic points along the pipeline. Ground beds induce a very small electrical charge into the soil, impeding the flow of electrons to the pipe. Pipeline personnel check the rectifier that induces the current into the ground bed on a regular basis to ensure that the system is applying sufficient current to maintain cathodic protection to the pipeline. A single 200-foot ground bed can protect as much as 50 miles of pipeline, but the low voltage used does not harm animals or plants in the vicinity.

The U.S. Department of Transportation (DOT) requires placement of aboveground signs to indicate the location of underground pipelines. These signs indicate the presence, location, product carried, and the name and contact information of the company that operates the pipeline. Markers are posted along the pipeline right-of-way (ROW) as well as at road, railroad, and waterway crossings. They are generally yellow, black, and red in color. Examples of pipeline markers are shown in Figure 3.



Painted Metal or Plastic Posts | Sign Located near Roads, Railroads, and along Pipeline Rights-of-Way | Pipeline Casing Vent | Marker for Pipeline Patrol Plane

Figure 3 Examples of Pipeline Identification Markers

Pipeline can be a vulnerable target because it is located outdoors, often in remote areas. Pipeline control systems are used to remotely monitor pipeline operations and can provide alarms when

off-normal conditions occur, such as during a leak. The pipeline ROW is not protected by a dedicated security force but is visually inspected by aerial patrols, usually biweekly.

Pump Stations

Oil and refined products are generally propelled through pipelines by centrifugal pumps. The pumps are sited at the originating station of the line and at booster stations every 20 to 100 miles along the length of the pipeline, depending on pipeline design, topography, and capacity requirements. Most pumps are driven by electric motors, although diesel engines or gas turbines can also be used.

Originating stations are more complex and have more equipment than booster stations. Pump stations typically include pumps, metering equipment, a complex array of piping and manifolds, supervisory control and data acquisition (SCADA) equipment, and scraper traps. Scraper traps are fixtures where pipeline cleaning and inspection devices, known as "pigs," are removed. Major stations, where custody of the fluid is transferred from one owner to another, contain a meter prover to calibrate metering equipment. Originating stations can also have storage tanks to smooth out variations in flow to the station, so pumps will operate continuously at near-normal capacity, even when small changes in crude or product supply occur. Figure 4 shows the inside of a typical pump station.

Figure 4 Inside View of a Pipeline Pump Station

Many feel that pumping stations are the most vulnerable component of a petroleum pipeline system. These stations are often in remote locations, unguarded, and unmanned. A General

Accounting Office report found that minor damage, such as pipe breaks, can be repaired very quickly, but the time to repair complex facilities (e.g., pump station) may extend beyond 6 months.

Storage Facilities

Storage facilities (storage fields and tank farms) are an important element in all pipeline systems. Storage allows flexibility in pipeline operations and minimizes unwanted fluctuations in pipeline throughput and product delivery. Both above- and belowground storage can be used.

Aboveground storage tanks are cylindrical and operated at near atmospheric pressure. Small, leased tanks are shop-fabricated and delivered to the site, where they are connected to pumps and other facilities. Large storage tanks may have a capacity of several hundred thousand barrels each and must be built on site. They often have a floating roof that moves up and down with the liquid level in the tank to minimize vapor losses. Smaller storage tanks have fixed roofs. Many crude oil storage tanks are equipped with vapor recovery systems to capture light hydrocarbons that evaporate from the crude and would otherwise be lost to the atmosphere. Figure 5 is a picture of a typical petroleum storage tank farm.

Figure 5 Typical Petroleum Storage Tank Farm

Storage tanks are constructed to withstand a certain amount of punishment, such as being rammed by a truck, but they can easily be ruptured with a powerful charge of explosives. Although tank farms are typically enclosed inside a security fence, they are highly visible, often unguarded, and can make for ready targets.

Block Valve Stations

Block valve stations are required on both sides of pump stations and at major waterways. The station contains a large, heavy-duty valve that is used to mechanically block flow through the pipeline during maintenance activities and emergencies. Block valve stations are installed on

trunk lines every 5 to 20 miles. Block valve stations are enclosed inside a security fence but are not manned and may be located in remote areas. Figure 6 shows a typical block valve station.

Figure 6 Typical Block Valve Station and Enclosure

Control Centers

Some pipeline systems have separate control centers for various pipeline segments, while other systems consolidate control of all pipeline segments into one central control center. Pipeline control rooms utilize SCADA systems that return real-time information about the rate of flow, the pressure, the speed, and other characteristics. SCADA systems continuously monitor, transmit, and process pipeline information for the control room dispatcher. Equipment status scans are taken every 5 to 20 seconds, depending on the communications technology used.

Monitoring is conducted by using remote terminal units (RTUs), which are placed at intervals along the pipeline and at associated facilities, such as pump stations and delivery terminals. RTUs periodically collect data from field instruments, which measure pressure, temperature, flow, and product density. RTUs can also receive information from vapor detectors and tank level gauges in pipeline system routing and storage areas. RTUs process this information to varying degrees and transmit it for analysis to a central computer through a communications network. Information from RTUs can be transmitted by company-owned lines, by a commercial telephone service, or by use of ground- or satellite-based microwave or radio communication.

Both computers and trained operators evaluate the information continuously. Most pipelines are operated and monitored 365 days a year, 24 hours per day. SCADA systems allow operators to shut down pipeline systems quickly and safely during an accident. Some systems also have backup or redundant communication capabilities in the event that one telecommunication mode (e.g., the local telephone system) is temporarily down.

Standards and Regulations

The design, construction, operation, and maintenance of interstate liquid petroleum transmission pipelines are regulated by DOT's Office of Pipeline Safety (OPS) under the Pipeline Safety Act (49 USC Chapter 601). OPS has issued regulations under 49 CFR Parts 194, 195, and 199. If the transmission pipeline is an intrastate pipeline and the state has established an office overseeing pipeline safety, additional state regulatory requirements can apply. In some cases, states have received approval from the federal OPS to inspect interstate pipelines for compliance with federal pipeline safety regulations, although enforcement authority remains under the jurisdiction of the federal OPS to assure continuity in interstate commerce. Offshore pipelines (i.e., in the Gulf of Mexico) are regulated by the Minerals Management Service in the U.S. Department of the Interior.

In May 2001, OPS began to implement a new approach for overseeing the safety of the network of U.S. pipelines that transport oil and natural gas. Traditionally, OPS carried out its oversight responsibility by issuing minimum safety standards and enforcing them uniformly across all pipelines. To better focus on safety risks that are unique to individual pipelines, OPS had been exploring a risk-based approach for overseeing pipeline safety since the mid-1990s and is now implementing this approach. This initiative—termed "integrity management"—requires pipeline operators, in addition to meeting minimum safety standards, to develop programs to assess, evaluate, and mitigate any risks to pipeline segments where a leak or rupture could have significant consequences, such as near highly populated areas. To address security concerns after September 11, 2001, OPS advised pipeline operators to consider potential terrorist threats to their pipelines in their assessments of pipeline risks. In addition to the integrity management initiative, OPS is implementing several actions to collect better data on pipeline incidents to improve its oversight of the pipeline industry and help evaluate the performance of the integrity management approach.

Prior to constructing new oil pipelines, operators must work with both state and federal permitting agencies, which are responsible for protecting wetlands, wildlife, ecosystems, and drinking water resources. Spills or releases from pipelines are first handled by the company responsible, its response contractors, local fire and police departments, and local emergency response personnel. If the amount of the oil spill exceeds an established reporting trigger, the company responsible for the spill is required to notify the federal government's National Response Center. A federal on-scene coordinator is designated, who determines the status of the local response and monitors the situation to determine whether, or how much, federal involvement is necessary.

Whenever new pipe is installed in the ground, workers are protected by requirements of the federal Occupational Safety and Health Administration. Facilities that include pipeline terminals and tank farms fall under local requirements based on codes published by the National Fire Protection Association. The Federal Energy Regulatory Commission oversees any tariffs that the pipelines charge for transporting services.

In July 2002, the American Petroleum Institute (API) published *Guidelines for Developing and Implementing Security Plans for Petroleum Pipelines*. By developing a pipeline security plan, operators can improve the security of pipeline systems and develop the knowledge and processes for making security-related decisions. Pipeline operators have and will continue to:

- Identify and analyze actual and potential events that can result in pipeline security-related incidents. Identify the likelihood and consequence of such events.
- Provide an integrated means for examining and evaluating risks and selecting risk reduction actions.
- Establish and track the effectiveness of a security plan.
- Establish security conditions (using the national threat advisory system) and specific protective measures based on the threat level.

The security of pipeline facilities has also been considered in relationship to other energy assets. The petroleum industry as a whole published Security Guidance for the Petroleum Industry in close cooperation with the U.S. Department of Energy, the U.S. Coast Guard, and DOT.

In 1998, the U.S. pipeline industry launched a multicompany Joint Environmental and Safety Initiative under the auspices of the Association of Oil Pipe Lines (AOPL) and the API's Pipeline Committee. The purpose of the initiative is to make further improvements in spill and accident prevention. A fundamental step in making improvements has been to understand the industry's current record in these areas. One primary purpose of the industry initiative has been to compile the most reliable information on the industry's safety record to date, so that the industry and its regulators will have a benchmark by which they can measure future performance.

In 1999, oil pipeline members of the API and the AOPL began tracking pipeline industry environmental and safety performance under the Pipeline Performance Tracking System (PPTS). Participation in PPTS is voluntary and open to receipt of any operator incident and infrastructure information. The PPTS participants provide performance information for all the facilities they operate, whether those facilities fall under the regulatory oversight of the OPS or not.

CONSEQUENCE OF EVENT

Petroleum pipelines form the backbone of the crude oil and refined petroleum product transportation system, transporting over two-thirds of those commodities in the U.S. Petroleum refineries depend on pipelines to receive crude oil and ship intermediate and finished products. Users of finished products, including the military, also depend a great deal on pipelines. A pipeline failure could have severe economic, environmental, and human health consequences.

Pipelines, and specifically pumping stations, are vulnerable as a result of exposed, unguarded facilities; computerized operations; a limited number of experienced personnel; lack of available spare parts; and a large amount of readily available public information on pipeline operations. The industry can respond to relatively minor damage quickly. In response to routine disruptions, such as breaks, ruptures, or pump failures, petroleum products can be rerouted through branch pipelines. Alternate control facilities and manual operations can replace centralized computer facilities, but they operate in a much less efficient manner. In some cases, truck or rail can provide an alternative means of transportation for small quantities over short distances.

One of the greatest vulnerabilities of a pipeline system is the pumping station. Repairing a severely damaged or destroyed pumping station could take 6 months or more because of its complexity. For example, the explosion and fire that destroyed TAPS Pump Station No. 8 caused crude oil throughput to drop almost in half, from 1.2 to 0.7 million barrels per day, and, despite an intense effort, rebuilding the station took more than 9 months. A recent report indicated that destroying only three pumping stations along a particular large pipeline could possibly cripple or halt its use.

Disruption of the movement of crude oil into a large refinery as a result of damage to or the destruction of its supply pipeline could shut down the refinery. The loss of the refinery's total product slate or the loss of its capacity to produce certain specialty reformulated fuels could create fuel shortages or price spikes locally or even nationally.

Pipelines cross rivers either on a bridge or under the riverbed. Such crossings are highly vulnerable and difficult to repair. Dropping a bridge may not only sever a pipeline carried on it but may also stop navigation (including tankers and barges associated with an oil terminal or refinery), block traffic, and hinder the delivery of repair equipment.

Severe environmental consequences could occur from a large-scale break in a pipeline, particularly if it contaminates a public water supply. Cleaning up the contamination could cost many millions of dollars. Damage could be exacerbated if another infrastructure component, such as a bridge, were damaged along with the pipeline.

A fire or explosion associated with the pipeline failure could cause injury or death to neighboring residents and business employees. Some victims could experience persistent or long-term health effects or illnesses.

COMMON VULNERABILITIES

Critical infrastructures and key assets vary in many characteristics and practices relevant to specifying vulnerabilities. There is no universal list of vulnerabilities that applies to all assets of a particular type within an infrastructure category. Instead, a list of common vulnerabilities has been prepared, based on experience and observation. These vulnerabilities should be interpreted as possible vulnerabilities and not as applying to each and every individual facility or asset. The following is a list of common vulnerabilities found at petroleum pipelines.

Exhibit 1 Economic and Institutional Vulnerabilities	
Economic and institutional vulnerabilities are those that would have extensive national, regional, or industry-wide consequences if exploited by a terrorist attack.	
1	Disruption of the crude oil pipeline into a large refinery could shut down the refinery. The loss of the refinery's total product slate or the loss of its capacity to produce certain specialty reformulated fuels could create fuel shortages or price spikes locally or even nationally.
2	The petroleum industry is a critical U.S. infrastructure. Loss of petroleum products, as demonstrated in the late 1970s and early 1980s, greatly impacts other industries, infrastructures, and the national economy and security. Pipelines are a critical link in this infrastructure because they transport crude oil to facilities where it is processed into finished products (e.g., gasoline, heating oil, jet fuel) used by consumers.
3	The loss of a critical facility (such as a pumping station) has the potential to shut down or severely reduce the capacity of the pipeline for an extended period of time (possibly up to a year). Spare parts could be in short supply, and the number of experienced personnel could be limited.

Exhibit 2 Site-Related Vulnerabilities	
Site-related vulnerabilities are conditions or situations existing at a particular site or facility that could be exploited by a terrorist or terrorist group to do economic, physical, or bodily harm or to disable or disrupt facility operations or other critical infrastructures.	
Access and Access Control	
1	Public roads may be in close proximity to critical assets (e.g., storage tanks) or control centers, allowing easy access by a vehicle-borne explosive device.
2	Critical assets are sometimes close to the perimeter fence, allowing for a successful attack from outside the fence line.
3	Pipeline ROWs run along public roads and rail lines and also intersect with them. Pipelines could be heavily damaged or destroyed by explosives; pipe sections could be unbolted and separated; and the fuel could be ignited.
4	Gates and critical assets near the perimeter fence line are difficult to protect by barriers or other hardening equipment.
5	Pipeline locations are easily identified by aboveground markers.
	(Continued on next page.)

6	Enclosure of critical facilities or assets can be incomplete or inadequate (e.g., fencing may not be completely secured at the bottom or have gaps or holes).
7	Camera surveillance may not be directed to view access points and other critical points within or without the premises.
8	Entrances to critical assets within the facility (e.g., control rooms) may not have controlled access. Once inside the control center, an intruder may have access to anywhere.
9	Employee and visitor parking may be next to critical facilities (e.g., control center).
Operational Security	
10	Risk Management Plan information is publicly available. Worst-case scenarios for toxic and flammable release are readily available.
11	Limited background checks are conducted on employees and contractor personnel. Some states or even union contracts limit the use of background investigations.
12	There may be limited coordination among local, state, and federal agencies on roles or responsibilities.
13	Websites provide a lot of information on pipeline locations, critical assets, maps, and other operational data.
14	Hacking attempts can provide adversaries with additional information.
SCADA and Process Control	
15	Some pipeline companies lack security around servers and control rooms.
16	There is a potential for intruders to hack into SCADA/process control through an enterprise network.
17	There is a potential for controllers to cause an undesirable event.
18	Wireless communication devices, which are being implemented in pipeline SCADA/process control systems, add further information technology vulnerabilities.
19	Standardized systems (e.g., Windows) and protocols are being used such that a vulnerability exploited at one pipeline system is applicable at multiple pipelines.
20	Typically, there is no backup for the control center facility.
Emergency Planning and Preparedness	
21	Contingency plans are not always formalized or exercised.
22	Limited emergency operation center backup facilities may be in place.
23	Spare parts that are large and/or expensive are in short supply. Economic considerations have reduced these spare part inventories. Lead times for obtaining some parts are long; some parts are available only from overseas vendors.
24	Aboveground pipelines can be attacked to cause fires or explosions.
25	Nontraditional fires or explosions can be created, which present additional challenges to first responders.
26	Coordination of emergency plans with industry neighbors and the local, state, and federal government may not always be compr3hensive.
Hazardous and Toxic Materials	
27	Because of the volatile nature of the products being transported, the destruction of almost any pipeline section or storage tank could create large fires.
28	Pipeline fires could release toxic materials.

Exhibit 3 Interdependent Vulnerabilities

Interdependency is the relationship between two or more infrastructures by which the condition or functionality of each infrastructure is affected by the condition or functionality of the other(s). Interdependencies can be physical, geographic, logical, or information-based.

Natural Gas/Fuel Oil	
1	Loss of natural gas or fuel oil can shut down pumping stations that use this fuel to drive the pumps.
2	Signs and valves used to identify natural gas ROWs and other aboveground equipment are visible and detectable.
Electric Power	
3	Loss of electric power could shut down pumping stations that use electricity to operate pumps.
4	Electric substations are generally unmanned and remote and so can be easily accessed.
5	Electric substations are easily identified by the entry and exit of large high-voltage wires.
6	Although usually enclosed by a fence, critical equipment at electric substations can be easily identified from off site.
7	Electric substations are usually surrounded by property belonging to third parties; therefore, the owner electric utility has little or no control or cooperation.
8	At electric substations, a long lead time is needed to obtain replacement transformers because of the wide diversity in transformers installed at substations throughout a utility's service territory. Depending on the date of installation and the function at the substation, some transformers are unique compared with the remainder of the utility's transformer inventory.
9	An inventory of large spare transformers required for critical high-voltage electric substations is not usually maintained because of cost.
10	Fire responders would not usually extinguish fires from electrical equipment because they would not have sufficient equipment or materials (e.g., aqueous film-forming foam [AFFF]) to fight a large electrical fire.
11	All key assets in electric substations and switching yards can be destroyed with small amounts of explosives.
12	Electric utility transmission lines and support towers are the most identifiable and vulnerable components in the system because of their remote and easily accessed locations.
Telecommunications	
13	Handheld radios may be critical to pipeline operations. Disruption of communications could reduce or stop pipeline throughput, which could severely disrupt downstream activities, such as refining or product delivery.
	(Continued on next page.)

14	Pipeline companies can have many hundreds of handheld radios. It is difficult to prevent their theft.
15	Adversaries can scan frequencies to determine operating conditions, the locations of employees and on-going activities, etc.
16	Communication with first responders is crucial to react in a timely manner to incidents. Jamming or other methods can be used to disrupt communication channels.
17	Telecommunications rely on a public switch network. Telephone congestion may occur during emergencies.

USEFUL REFERENCE MATERIALS AND WEBSITES

Allegro Energy Group, *How Pipelines Make the Oil Market Work – Their Networks, Operation and Regulation*, A Memorandum Prepared for the Association of Oil Pipe Lines and the American Petroleum Institute's Pipeline Committee, December 2001 [http://www.pipeline101.com/reports/Notes.pdf].

American Petroleum Institute Website [http://api-ep.api.org/].

Association of Oil Pipelines Website [http://www.aopl.org/default.asp].

Goen, Richard L., Richard B. Bothun, and Frank E. Walker, *Potential Vulnerabilities Affecting National Survival*, Stanford Research Institute report to the Office of Civil Defense, Department of the Army, OCD Work Unit 3535A, contract DAHC 20-69-C-0186, Stanford, CA, Sept. 1970.

Kennedy, John L., *Oil and Gas Pipeline Fundamentals*, 2nd edition, PennWell Publishing Company, Tulsa, OK, 1993.

Pipeline 101 Website [http://www.pipeline101.com/index.html].

Pipeline Safety Foundation Website [http://www.pipelinesafetyfoundation.org/index.shtml].

U.S. Department of Transportation, Pipeline Safety Division [http://www.tsi.dot.gov/divisions/pipeline/pipeline.htm].

Wuesthoff, S.E., *The Utility of Targeting the Petroleum-based Sector of a Nation's Economic Infrastructure* [http://www.maxwell.af.mil/au/aul/aupress/SAAS_Theses/Wuesthoff/wuesthoff.pdf].