POTENTIAL INDICATORS OF TERRORIST ACTIVITY INFRASTRUCTURE CATEGORY: PETROLEUM PIPELINES

Protective Security Division
Department of Homeland Security

Draft – Version 1, March 5, 2004

Preventing terrorism and reducing the nation's vulnerability to terrorist acts require identifying specific vulnerabilities at critical sites, understanding the types of terrorist activities—and the potential indicators of those 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 discusses potential indicators of terrorist activity with a focus on petroleum pipelines.

INTRODUCTION

Terrorist activity indicators are observable anomalies or incidents that may precede a terrorist attack or that may be associated with terrorist surveillance, training, planning, preparation, or mobilization activities. The observation of any one indicator may not, by itself, suggest terrorist activity. Each observed anomaly or incident, however, should be carefully considered, along with all other relevant observations, to determine whether further investigation is warranted. The objective is to look for items of information that fit together to form a relevant and credible picture of how a threat might become real at the petroleum pipelines of interest and what it might look like. The key factor in early recognition of terrorist activity is the ability to recognize anomalies in location, timing, and character of vehicles, equipment, people, and packages.

The geographic location and temporal proximity (or dispersion) of observed anomalies are important factors to consider. Terrorists have demonstrated the ability to finance, plan, and train for complex and sophisticated attacks over extended periods of time and at multiple locations distant from the proximity of their targets. Often, attacks are carried out nearly simultaneously against multiple targets.

Indicators are useful in discerning terrorist activity to the extent that they help identify:

- A specific asset that a terrorist group is targeting,
- The general or specific timing of a planned attack, and
- The weapons and deployment method planned by the terrorist.

In some cases, the choice of weaponry and deployment method may help to eliminate certain classes of assets from the potential target spectrum. Except for geographic factors, however, such

information alone may contribute little to identifying the specific target or targets. The best indicator that a specific site or asset may be targeted is direct observation or evidence that the site or asset is or has been under surveillance. Careful attention to the surveillance indicators, especially by local law enforcement personnel and asset owners, is an important key to identifying potential terrorist threats to a specific site or asset. To increase the probability of detecting terrorist surveillance activities, employees, contractors, and local citizens need to be solicited to "observe and report" unusual activities, incidents, and behaviors highlighted in this report.

PETROLEUM PIPELINES BACKGROUND

Terrorist Targeting Objectives

Figure 1 depicts the range of possible objectives for a terrorist attack on petroleum pipelines. Inflicting casualties in the form of fatalities, injuries, and illnesses is one of the major objectives of many terrorist acts. Casualties can occur both at the facility and in the surrounding area. Damage or destruction of the facility can be intended to shut down or degrade the operation of the facility, or to cause the release of hazardous materials to the surrounding area. Disruption of the facility without inflicting actual damage can be intended to interfere with facility operations and cause a decrease of output or to tamper with facility products to render them dangerous or unusable. Theft of equipment, materials, or products can be intended to divert these items to other uses or reap financial gain from their resale. Theft of information can be intended to acquire insight that is not made public or gain data that can be used in carrying out attacks.

Specific threats that are of concern to petroleum pipelines include:

- Explosives (e.g., car bomb, suicide bomber),
- Stand-off weapons (e.g., rocket-propelled grenade), and
- Malicious control of equipment (e.g., through a supervisory control and data acquisition [SCADA] system).

Characterization of the Industry

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 ocean tankers and barges, which account 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 2 and 3 are maps of the network of crude oil and refined product pipelines in the U.S., respectively.

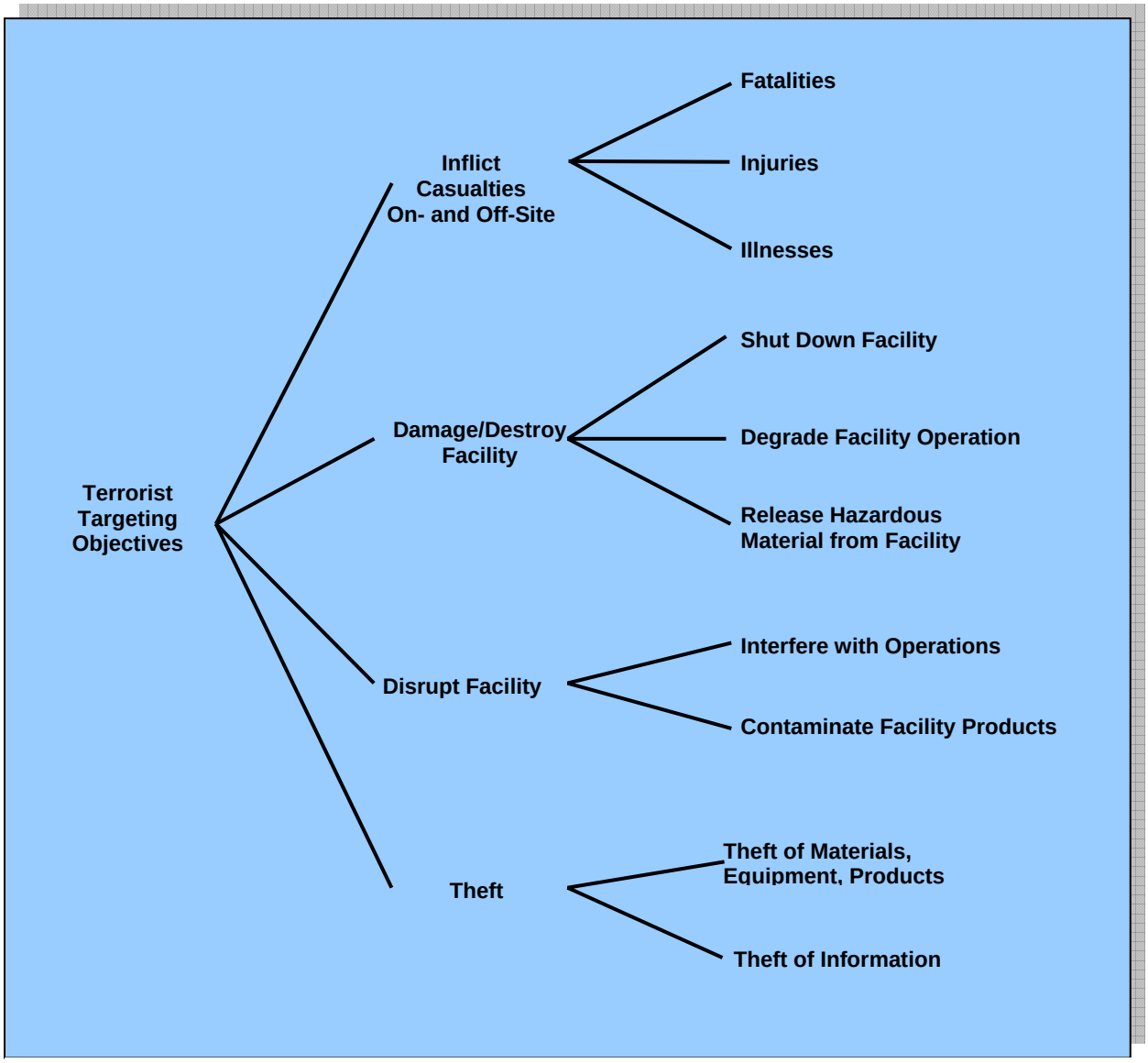

Figure 1 Potential Terrorist Targeting Objectives

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, they 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.

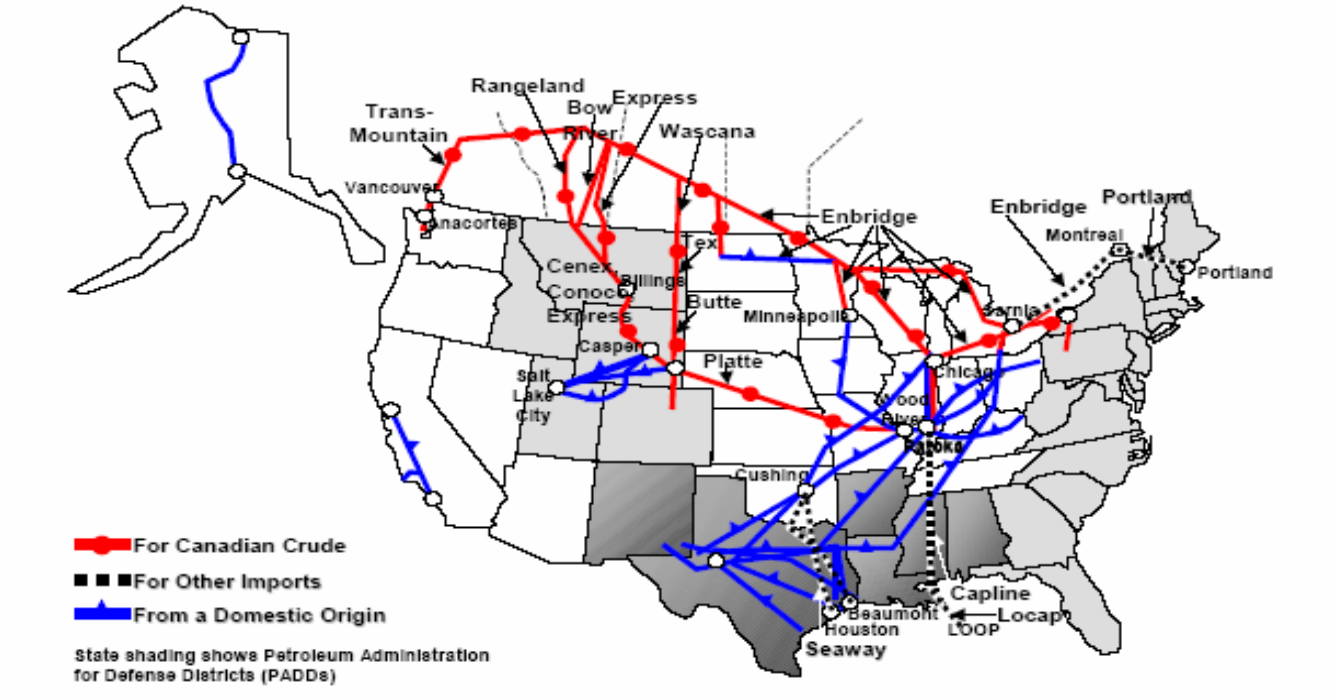

Figure 2 Crude Oil Pipeline Network

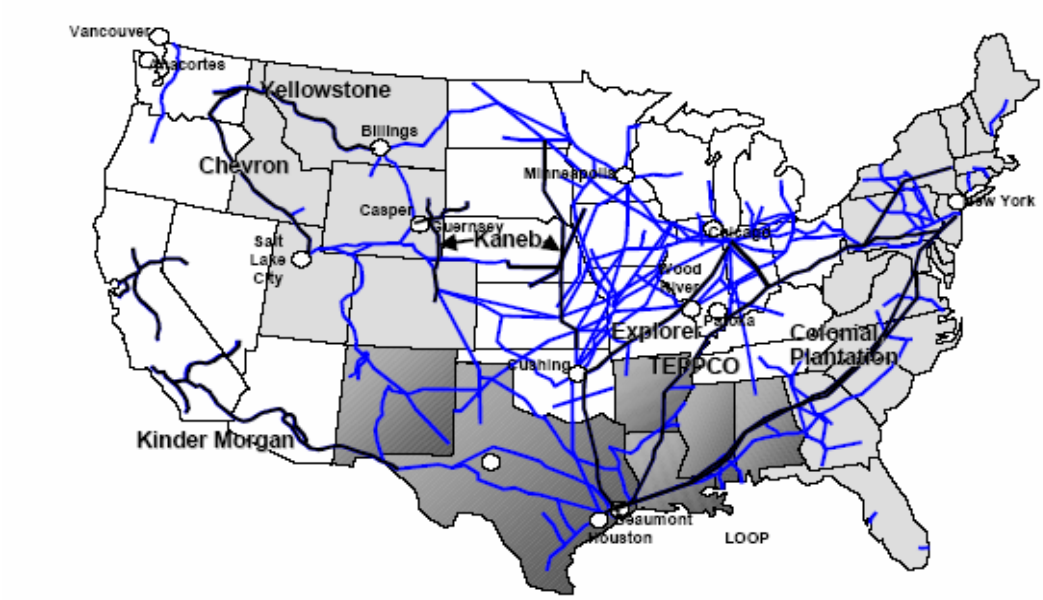

Figure 3 Refined Product Pipeline Network

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 to 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 3). 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 Facility Characteristics

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 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 4.

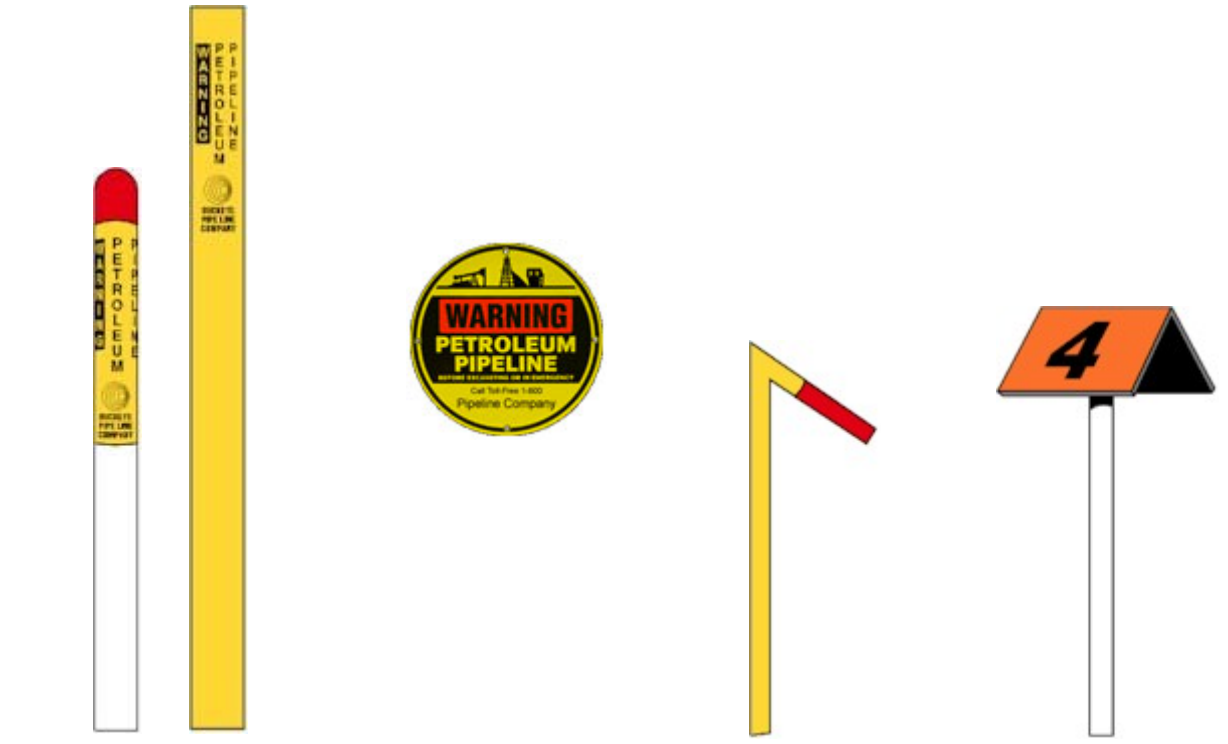

Figure 4 Examples of Pipeline Identification Markers

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, 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 5 shows the inside of a typical pump station.

Figure 5 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 stations) may extend beyond six 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 below-ground 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 6 is a picture of a typical petroleum storage tank farm.

Figure 6 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 7 shows a typical block valve station.

Figure 7 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, a commercial telephone service, or 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.

TERRORIST ACTIVITY INDICATORS

There are several indicators of possible terrorist activity that should be monitored regularly. Constant attention to these indicators can help alert officials to the possibility of an incident.

Surveillance Indicators

Terrorist surveillance may be fixed or mobile. Fixed surveillance is done from a static, often concealed position, possibly an adjacent building, business, or other facility. In fixed surveillance scenarios, terrorists may establish themselves in a public location over an extended period of time or choose disguises or occupations such as street vendors, tourists, repair or deliverymen, photographers, or even demonstrators to provide a plausible reason for being in the area.

Mobile surveillance usually entails observing and following persons or individual human targets, although it can be conducted against nonmobile facilities (i.e., driving by a site to observe the facility or site operations). To enhance mobile surveillance, many terrorists have become more adept at progressive surveillance.

Progressive surveillance is a technique whereby the terrorist observes a target for a short time from one position, withdraws for a time (possibly days or even weeks), and then resumes surveillance from another position. This activity continues until the terrorist develops target suitability and/or noticeable patterns in the operations or target's movements. This type of transient presence makes the surveillance much more difficult to detect or predict.

More sophisticated surveillance is likely to be accomplished over a long period of time. This type of surveillance tends to evade detection and improve the quality of gathered information. Some terrorists perform surveillance of a target or target area over a period of months or even years. The use of public parks and other public gathering areas provides convenient venues for surveillance because it is not unusual for individuals or small groups in these areas to loiter or engage in leisure activities that could serve to cover surveillance activities.

Terrorists are also known to use advanced technology such as modern optoelectronics, communications equipment, video cameras, and other electronic equipment. Such technologies include commercial and military night-vision devices and global positioning systems. It should be assumed that many terrorists have access to expensive technological equipment.

Electronic surveillance, in this instance, refers to information gathering, legal and illegal, by terrorists using off-site computers. This type of data gathering might include site maps, key facility locations, site security procedures, or passwords to company computer systems. In addition to obtaining information useful for a planned physical attack, terrorists may launch an electronic attack that could affect data (e.g., damage or modify), software (e.g., damage or

modify), or equipment/process controls (e.g., damage a piece of equipment or cause a dangerous chemical release by opening or closing a valve using off-site access to the SCADA system). Terrorists may also use technical means to intercept radio or telephone (including cell phone) traffic.

An electronic attack could be an end in itself or could be launched simultaneously with a physical attack. Thus, it is worthwhile to be aware of what information is being collected from company and relevant government websites by off-site computer users and, if feasible, who is collecting this information. In addition, it is also important to know whether attempts are being made to gain access to protected computer systems and whether any attempts have been successful.

The surveillance indicators in Exhibit 1 are examples of unusual activities that should be noted and considered as part of an assimilation process that takes into account the quality and reliability of the source, the apparent validity of the information, and how the information meshes with other information at hand. For the most part, surveillance indicators refer to activities in the immediate vicinity of the facility; most of the other indicator categories in this report address activities in a much larger region around the facility.

Other Local and Regional Indicators

The remaining sets of indicators described in Exhibits 2 to 5 refer to activities not only in the immediate vicinity of the facility, but also activities within a relatively large region around the facility (e.g., 100 to 200 miles). Local authorities should be aware of such activities and may not be able to associate them with a specific critical asset because several may be within the region being monitored. The objective is to look for items of information that fit together to form a relevant and credible picture of how a threat might become real at the facility of interest and what it might look like.

EXHIBITS

Every attempt has been made to be as comprehensive as possible in listing the following terrorist activity indicators. Some of the indicators listed may not be specific to the critical infrastructure or critical asset category that is the topic of this report. However, these general indicators are included as an aid and reminder to anyone who might observe any of these activities that they are indicators of potential terrorist activity.

Exhibit 1 Surveillance Indicators Observed Inside or Outside an Installation

What are surveillance indicators? Persons or unusual activities in the immediate vicinity of a critical infrastructure or key asset intending to gather information about the facility or its operations, shipments, or protective measures.

Persons Observed or Reported:

1	Persons using or carrying video/camera/observation equipment.
2	Persons with installation maps or facility photos or diagrams with facilities highlighted or notes regarding infrastructure or listing of installation personnel.
3	Persons possessing or observed using night-vision devices near the facility perimeter or in the local area.
4	Persons parking, standing, or loitering in the same area over a multiple-day period with no apparent reasonable explanation.
5	Non-military persons seen with military-style weapons and clothing/equipment.
6	Facility personnel being questioned off-site about practices pertaining to the facility, or an increase in personal e-mail, telephone, faxes, or mail concerning the facility or key asset.
7	Non-facility persons showing an increased general interest in the area surrounding the facility.
8	Facility personnel willfully associating with suspicious individuals.
9	Computer hackers attempting to access sites looking for personal information, maps, or other targeting examples.
10	An employee who changes working behavior or works more irregular hours.
11	Persons observed or reported to be observing facility receipts or deliveries, especially of hazardous, toxic, or radioactive materials.
12	Aircraft flyover in restricted airspace; boat encroachment into restricted areas, especially if near critical infrastructure.
	(Continued on next page.)

Activities Observed or Reported:	
13	A noted pattern or series of false alarms requiring a response by law enforcement or emergency services.
14	Theft of facility or contractor identification cards or uniforms, or unauthorized persons in possession of facility ID cards or uniforms.
15	Recent damage (e.g., significant holes or cuts) to a perimeter fence or gate, or damage to perimeter lighting, security cameras, motion sensors, guard dogs, or other security devices.
16	Downloading of materials (e.g., maps, photographs, schematics, or similar materials) that could be used in conjunction with surveillance or attack planning activities.
17	Repeated attempts from the same location or country to access protected computer information systems.
18	Successful penetration and access of protected computer information systems, especially those containing information on site logistics, procedures, shipment schedules, security measures, passwords, and other sensitive information.
19	Attempts to obtain information about the facility (e.g., blueprints of buildings or information from public sources).
20	Unfamiliar cleaning crews or other contract workers with passable credentials; crews or contract workers attempting to access unauthorized areas.
21	A seemingly abandoned or illegally parked vehicle in the area of the facility or asset.
22	Increased interest in facility outside components (i.e., an electrical substation not located on site and not as heavily protected or not protected at all).
23	Sudden increases in power outages. This could be done from an off-site location to test the backup systems or recovery times of primary systems.
24	Increase in buildings being left unsecured or doors being left unlocked that are normally locked all the time.
25	Arrest by local police of unknown persons. This would be more important if the facility or asset is located in a rural area rather than located in or around a large city.
26	Traces of explosive or radioactive residue on facility vehicles during security checks by personnel using detection swipes or devices.
27	Increase in violation of security guard standard operating procedures for staffing key posts.
28	Increase in threats from unidentified sources by telephone, postal mail, or through the e-mail system.
29	Increase in reports of threats from outside known, reliable sources.
30	Sudden losses or theft of guard force communications equipment.
31	Displaced or misaligned manhole covers or other service access doors on or surrounding the facility or asset site.
32	Unusual maintenance activities (e.g., road repairs) near the facility or asset.
33	Observations of unauthorized facility or non-facility personnel collecting or searching through facility trash.

Exhibit 2 Transactional and Behavioral Indicators

What are transactional and behavioral indicators? Suspicious purchases of materials for improvised explosives or for the production of biological agents, toxins, chemical precursors, or chemicals that could be used in an act of terrorism or for purely criminal activity in the immediate vicinity or in the region surrounding a facility, critical infrastructure, or key asset.

Transactional Indicators:

What are transactional indicators? Unusual, atypical, or incomplete methods, procedures, or events associated with inquiry about or attempted purchase of equipment or materials that could be used to manufacture or assemble explosive, biological, chemical, or radioactive agents or devices that could be used to deliver or disperse such agents. Also included are inquiries and orders to purchase such equipment or materials and the subsequent theft or loss of the items from the same or a different supplier.

1	Approach from a previously unknown customer or vendor (including those who require technical assistance) whose identity is not clear.
2	Transaction involving an intermediary agent and/or third party or consignee that is atypical in light of his/her usual business.
3	A customer or vendor associated with or employed by a military-related business, such as a foreign defense ministry or foreign armed forces.
4	Unusual customer or vendor request concerning the shipment or labeling of goods (e.g., offer to pick up shipment personally rather than arrange shipment and delivery).
5	Packaging and/or packaging components that are inconsistent with the shipping mode or stated destination.
6	Unusually favorable payment terms, such as a higher price or better interest rate than the prevailing market or a higher lump-sum cash payment.
7	Unusual customer or vendor request for excessive confidentiality regarding the final destination or details of the product to be delivered.
8	Orders for excessive quantities of personal protective gear or safety/security devices, especially by persons not identified as affiliated with an industrial plant.
9	Requests for normally unnecessary devices (e.g., an excessive quantity of spare parts) or a lack of orders for parts typically associated with the product being ordered, coupled with an unconvincing explanation for the omission of such an order or request.
10	Sale canceled by customer but then customer or vendor attempts to purchase or sell the exact same product with the same specifications and use but using a different name.
11	Sale canceled by customer or vendor but then the identical product is stolen or “lost” shortly after the customer’s or vendor’s inquiry.
12	Theft/loss/recovery of large amounts of cash by groups advocating violence against government/civilian sector targets (also applies to weapons of mass destruction).
	(Continued on next page.)

13	Customer or vendor does not request a performance guarantee, warranty, or service contract where such is typically provided in similar transactions.
Customer/Vendor Behavioral Indicators: *What are customer or vendor behavioral indicators? Actions or inactions on the part of a customer or vendor for equipment or materials that appear to be inconsistent with normal behavioral patterns expected from legitimate commercial activities.*	
14	Reluctance to give sufficient explanation of the materials to be produced with the equipment and/or the purpose or use of those materials.
15	Evasive responses.
16	Reluctance to provide information on the locations or place where the equipment is to be installed.
17	Reluctance to explain sufficiently what raw materials are to be used with the equipment.
18	Reluctance to provide clear answers to routine commercial or technical questions.
19	Reason for purchasing the equipment does not match the customer's or vendor's usual business or technological level.
20	No request made or declines or refuses technical expert/training assistance when the assistance is generally standard for the installation or operation of the equipment.
21	Unable to complete an undertaking (due to inadequate equipment or technological know-how) and requests completion of a partly finished project.
22	Plant, equipment, or item is said to be for a use inconsistent with its design or normal intended use, and the customer or vendor continues these misstatements even after being corrected by the company/distributor.
23	Contract provided for the construction or revamping of a plant, but the complete scope of the work and/or final site of the plant under construction is not indicated.
24	Theft of material or equipment with no practical use outside of a legitimate business facility or industrial process.
25	Apparent lack of familiarity with nomenclature, processes, packaging configurations, or other indicators to suggest this person may not be routinely involved in the business.
26	Discontinuity of information provided, such as a phone number for a business, but the number is listed under a different name.
27	Unfamiliarity with the "business," such as predictable business cycles, etc.
28	Unreasonable market expectations or fantastic explanations as to where the end product is going to be sold.

Exhibit 3 Weapons Indicators

What are weapons indicators? Purchase, theft, or testing of conventional weapons and equipment that terrorists could use to help carry out the intended action. Items of interest include not only guns, automatic weapons, rifles, etc., but also ammunition and equipment, such as night-vision goggles and body armor and relevant training exercises and classes.

Activities Observed or Reported:	
1	Theft or sales of large numbers of automatic or semi-automatic weapons.
2	Theft or sales of ammunition capable of being used in military weapons.
3	Reports of automatic weapons firing or unusual weapons firing.
4	Seizures of modified weapons or equipment used to modify weapons (silencers, etc.).
5	Theft, loss, or sales of large-caliber sniper weapons .50 cal or larger.
6	Theft, sales, or reported seizure of night-vision equipment in combination with other indicators.
7	Theft, sales, or reported seizure of body armor in combination with other indicators.
8	Paramilitary groups carrying out training scenarios and groups advocating violence.
9	People wearing clothing that is not consistent with the local weather (also applicable under all other indicator categories).

Exhibit 4 Explosive and Incendiary Indicators

What are explosive and incendiary indicators? Production, purchase, theft, testing, or storage of explosive or incendiary materials and devices that could be used by terrorists to help carry out the intended action. Also of interest are containers and locations where production could occur.

Persons Observed or Reported:	
1	Persons stopped or arrested with unexplained lethal amounts of explosives.
2	Inappropriate inquiries regarding explosives or explosive construction by unidentified persons.
3	Treated or untreated chemical burns or missing hands and/or fingers.
Activities Observed or Reported:	
4	Thefts or sales of large amounts of smokeless powder, blasting caps, or high-velocity explosives.
5	Large amounts of high-nitrate fertilizer sales to non-agricultural purchasers or abnormally large amounts to agricultural purchasers.[1]
6	Large thefts or sales of combinations of ingredients for explosives (e.g., fuel oil, nitrates) beyond normal.
7	Thefts or sales of containers (e.g., propane bottles) or vehicles (e.g., trucks, cargo vans) in combination with other indicators.
8	Reports of explosions, particularly in rural or wooded areas.
9	Traces of explosive residue on facility vehicles during security checks by personnel using explosive detection swipes or devices.
10	Seizures of improvised explosive devices or materials.
11	Purchase or theft of explosives or restricted or sensitive chemicals.
12	Theft of truck or van with minimum one-ton carrying capacity.
13	Modification of light-duty vehicle to accept a minimum one-ton load.
14	Rental of self-storage units and/or delivery of chemicals to such units.
15	Chemical fires, noxious or toxic odors, brightly colored stains, or rusted metal fixtures in apartments, hotel rooms, or self-storage units.
16	Suspicious packages, especially unexpected deliveries with no or an unknown return address and/or with excessive postage.
17	Unattended packages, briefcases, or other containers.
18	Unexpected or unfamiliar delivery trucks or deliveries.
19	Vehicles containing unusual or suspicious parcels or materials.
20	Unattended vehicles on- or off-site in suspicious locations or at unusual times.

[1] The Fertilizer Institute developed a "Know Your Customer" program following the terrorist incident at Oklahoma City. The information is available from TFI at http://www.tfi.org/.

Exhibit 5 Chemical, Biological, and Radiological Indicators

What are chemical, biological, and radiological indicators? Activities related to production, purchase, theft, testing, or storage of dangerous chemicals and chemical agents, biological species, and hazardous radioactive materials.

Equipment Configuration Indicators:	
1	Equipment to be installed in an area under strict security control, such as an area close to the facility or an area to which access is severely restricted.
2	Equipment to be installed in an area that is unusual and out of character with the proper use of the equipment.
3	Modification of a plant, equipment, or item in an existing or planned facility that changes production capability significantly and could make the facility more suitable for the manufacture of chemical weapons or chemical weapon precursors. (This also applies to biological agents and weapons.)
4	Suspicious packages, especially unexpected deliveries with no or an unknown return address and/or with excessive postage.
5	Unattended packages, briefcases, or other containers.
6	Unexpected or unfamiliar delivery trucks or deliveries.
7	Vehicles containing unusual or suspicious parcels or materials.
8	Theft, sale, or reported seizure of sophisticated personal protective equipment, such as “A”-level Tyvek, self-contained breathing apparatus (SCBA), etc.
9	Theft or sale of sophisticated filtering, air-scrubbing, or containment equipment.
Chemical Agent Indicators:	
10	Inappropriate inquiries regarding local chemical sales/storage/transportation points.
11	Purchase or theft of explosives or restricted or sensitive chemicals.
12	Rental of self-storage units and/or delivery of chemicals to such units.
13	Chemical fires, noxious or toxic odors, brightly colored stains, or rusted metal fixtures in apartments, hotel rooms, or self-storage units.
14	Treated or untreated chemical burns or missing hands and/or fingers.
15	Unusual packages or containers, especially near heating, ventilating, and air-conditioning (HVAC) equipment or air intake systems.
16	Unusual powders, droplets, or mist clouds near HVAC equipment or air-intake systems.
Biological Agent Indicators:	
17	Sales or theft of large quantities of baby formula (medium for growth), or an unexplained shortage of it.
18	Break-ins/tampering at water treatment or food processing/warehouse facilities.
	(Continued on next page.)

19	Solicitation for sales or theft of live agents/toxins/diseases from medical supply companies or testing/experiment facilities.
20	Persons stopped or arrested with unexplained lethal amounts of agents/toxins/ diseases/explosives.
21	Multiple cases of unexplained human or animal illnesses, especially those illnesses not native to the area.
22	Large number of unexplained human or animal deaths.
23	Sales (to non-agricultural users) or thefts of agricultural sprayers or crop-dusting aircraft, foggers, river craft (if applicable), or other dispensing systems.
24	Inappropriate inquiries regarding local or regional chemical/biological sales/storage/transportation points.
25	Inappropriate inquiries regarding heating and ventilation systems for buildings/facilities by persons not associated with service agencies.
26	Unusual packages or containers, especially near HVAC equipment or air-intake systems.
27	Unusual powders, droplets, or mist clouds near HVAC equipment or air-intake systems.
Radioactive Material Indicators:	
28	Break-ins/tampering at facilities storing radioactive materials or radioactive wastes.
29	Solicitation for sales or theft of radioactive materials from medical or research supply companies or from testing/experiment facilities.
30	Persons stopped or arrested with unexplained radioactive materials.
31	Any one or more cases of unexplained human or animal radiation burns or radiation sickness.
32	Large number of unexplained human or animal deaths.
33	Inappropriate inquiries regarding local or regional radioactive material sales/storage/transportation points.

USEFUL REFERENCE MATERIAL AND RELATED WEB SITES

1. White House, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets,* Feb. 2003 [http://www.whitehouse.gov/pcipb/physical.html].

2. *Terrorist Attack Indicators,* Html file: [http://afsf.lackland.af.mil/Organization/AFSFC/SFP/AF%20Pubs/Terrorist%20Attack%20Indicators]; PDF file: [http://216.239.53.100/search?q=cache:YMHxMOEIgOcJ:afsf.lackland.af.mil/Organization/AFSFC/SFP/AF%2520Pubs/Terrorist%2520Attack%2520Indicators.PDF+terrorist+attack+indicators&hl=en&ie=UTF-8].

3. U.S. Department of Homeland Security, "Potential Indicators of Threats Involving Vehicle-Borne Improvised Explosive Devices (VBIEDs)," *Homeland Security Information Bulletin,* May 15, 2003 [http://www.apta.com/services/security/potential_indicators.cfm]. This document includes a table of chemicals and other demolitions paraphernalia used in recent truck bomb attacks against U.S. facilities.

4. U.S. Federal Bureau of Investigation, *FBI Community Outreach Program for Manufacturers and Suppliers of Chemical and Biological Agents, Materials, and Equipment* [http://www.vohma.com/pdf/pdffiles/SafetySecurity/ChemInfofbi.pdf]. This document includes a list of chemical/biological materials likely to be used in furtherance of WMD terrorist activities.

5. Defense Intelligence College, Counterterrorism Analysis Course, *Introduction to Terrorism Intelligence Analysis, Part 2: Pre-Incident Indicators* [http://www.globalsecurity.org/intell/library/policy/dod/ct_analysis_course.htm].

6. Princeton University, Department of Public Safety, *What is a Heightened Security State of Alert?* [http://web.princeton.edu/sites/publicsafety/].

7. Kentucky State Police: Homeland Security/Counter-Terrorism, *Potential Indicators of WMD Threats or Incidents* [http://www.kentuckystatepolice.org/terror.htm]. This site lists several indicators, protective measures, and emergency procedures.

8. U.S. Air Force, Office of Special Investigations, *Eagle Eyes: Categories of Suspicious Activities* [http://www.dtic.mil/afosi/eagle/suspicious_behavior.html]. This site has brief descriptions of activities such as elicitation, tests of security, acquiring supplies, suspicious persons out of place, dry run, and deploying assets.

9. Baybutt, Paul, and Varick Ready, "Protecting Process Plants: Preventing Terrorism Attacks and Sabotage," *Homeland Defense Journal,* Vol. 2, Issue 3, pp. 1–5, Feb. 12, 2003 [http://www.homelanddefensejournal.com/archives/pdfs/Feb_12_vol2_iss3.pdf].

10. U.S. Department of Homeland Security [http://www.dhs.gov/dhspublic/index.jsp].

11. Federal Bureau of Investigation [http://www.fbi.gov/].

12. Agency for Toxic Substances and Disease Registry [http://www.atsdr.cdc.gov/].

13. Centers for Disease Control and Prevention [http://www.cdc.gov/].

14. U.S. Department of Commerce, Bureau of Industry and Security [http://www.bis.doc.gov/].

15. 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].

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

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

18. 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.

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

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

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

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

23. 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].