

## POTENTIAL INDICATORS OF TERRORIST ACTIVITY INFRASTRUCTURE CATEGORY: LNG IMPORT FACILITIES

Protective Security Division  
Department of Homeland Security

Version 3, December 9, 2003



*Preventing terrorism and reducing the nation's vulnerability to terrorist acts requires 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 liquefied natural gas (LNG) import facilities, which handle large quantities of flammable and potentially explosive LNG when vaporized under the right circumstances.*

### 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. However, each observed anomaly or incident 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 liquefied natural gas (LNG) import facility of interest and what it might look like. The key factor to 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. However, except for geographic factors, 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.

## **LIQUEFIED NATURAL GAS IMPORT FACILITY BACKGROUND**

### **Terrorists Targeting Objectives**

To consider terrorist threat indicators in relationship to LNG import facilities, it is useful to understand the basic structure of the industry and what general types of facilities might be attractive targets for terrorist attack. LNG import facilities may be attractive terrorist targets because

- Import facilities have large quantities of volatile, flammable LNG that could lead to spectacular fires and explosions,
- Large shipping vessels that deliver LNG are vulnerable to attack,
- Some regions of the United States (U.S.) rely on LNG imports for a significant share of their natural gas supply, so an extended outage or outages could lead to severe economic disruptions.

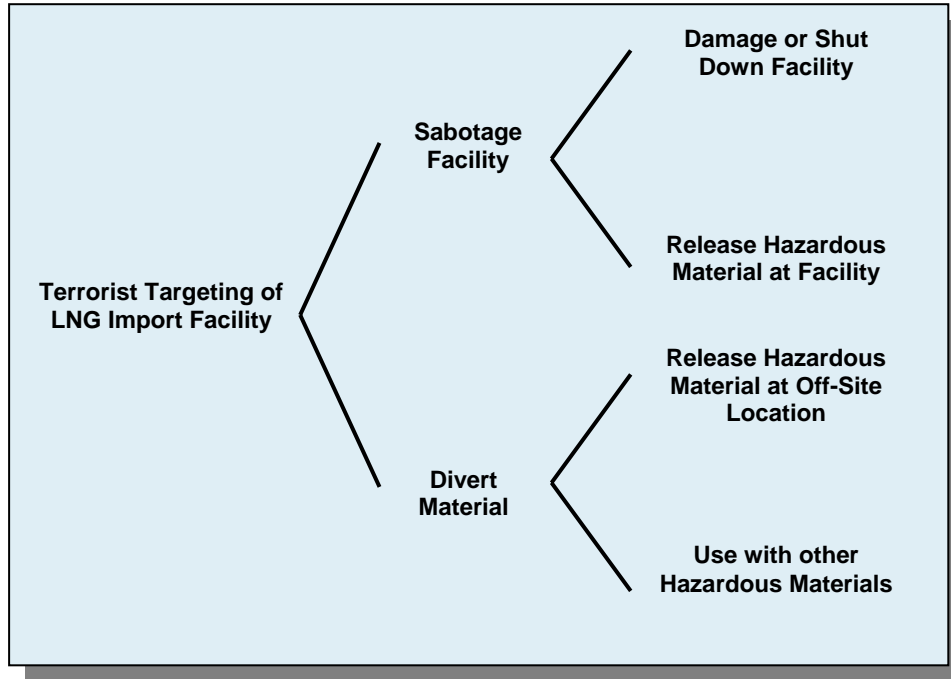
Generally speaking, terrorists or terrorist groups may target LNG import facilities or tankers to either (1) sabotage the facility, or, in what seems to be a much less likely possibility, (2) divert LNG for other purposes, as depicted in Figure 1. Facility sabotage can be to “weaponize” the facility against the surrounding population by causing the uncontrolled release of LNG from the facility and causing a subsequent fire. Facility sabotage might also be used to cause economic, national security, or logistical harm.

### **Sector Description**

LNG is natural gas (primarily methane) that has been liquefied by reducing its temperature to -260 degrees Fahrenheit at atmospheric pressure. After LNG is converted back to natural gas, it can be injected into natural gas pipelines and distributed in the usual way.

The U.S. has been importing increasing volumes of LNG, exceeding 238 Bcf in 2001. As recently as 1996, imports were only 40 Bcf. The total LNG imports in 2001 represent about 6% of total U.S. imports of natural gas and only about 1% of U.S. natural gas consumption. In 2001, the U.S. imported LNG from six countries, as shown in Table 1. On a regional and seasonal

basis, however, LNG is becoming an important source of natural gas. The U.S. also has a liquefaction plant in Alaska and exports LNG to Japan; a total of 66 Bcf of LNG was exported in the year 2000.<sup>15</sup>



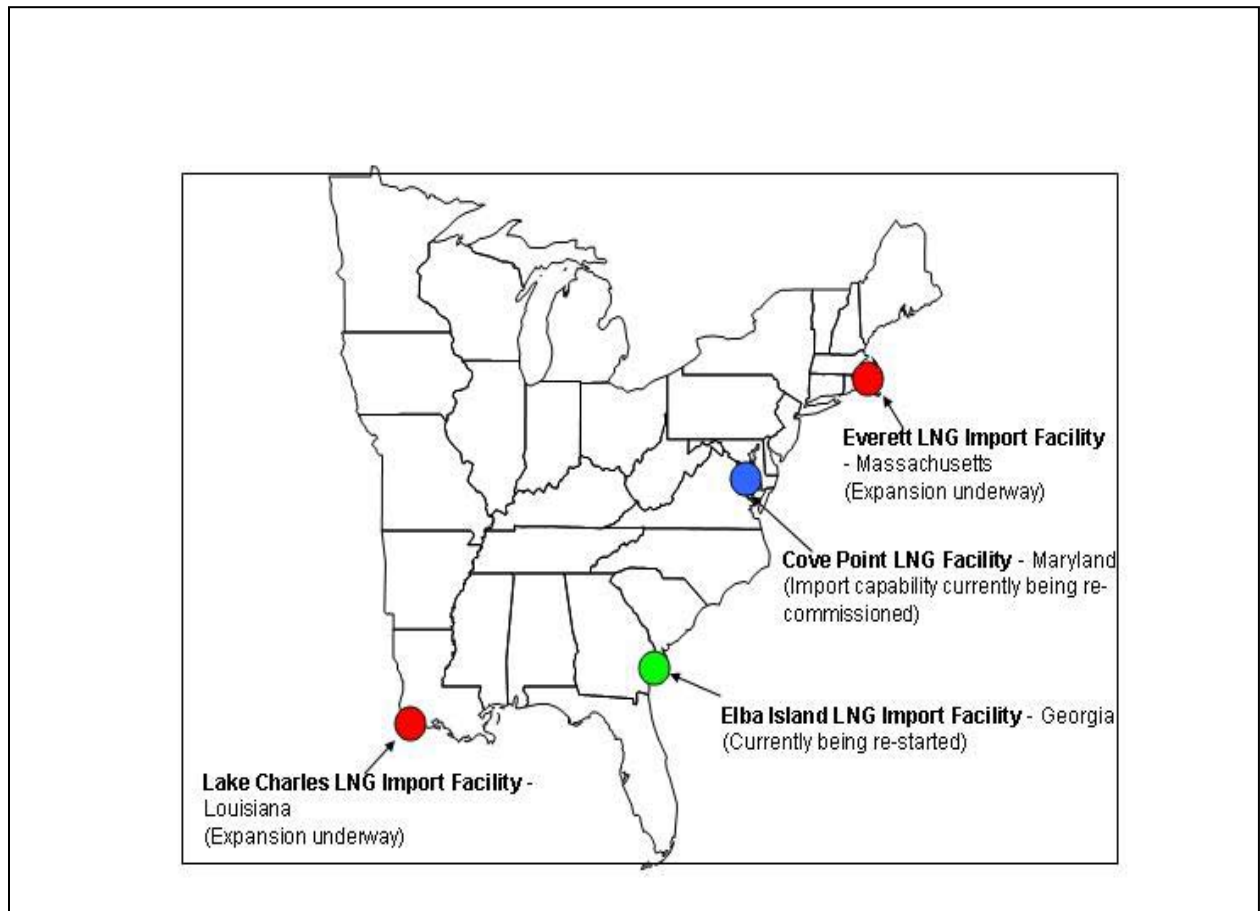
**Figure 1 Terrorist Targeting Objectives for LNG Import Facilities**

The method of transporting and receiving LNG makes this energy source a matter of concern for infrastructure protection. The intensely cold LNG has a volume that is 620 times smaller than the original gas. LNG is transported at atmospheric pressure in special, heavily insulated cryogenic tankers to a marine terminal, where it is stored in insulated tanks. When needed, LNG can be piped to a nearby gasification plant, where it is vaporized and then distributed to customers by pipeline, similar to wellhead gas.

On October 12, 2001, the U.S. Coast Guard lifted the ban on LNG tankers from Boston Harbor. The ban, which had been in effect since September 26 (two weeks after the terrorist attacks in New York and Washington, D.C.), was established in response to security and safety concerns about the ships that transport LNG to the import facility of Distrigas of Massachusetts (a Division of Tractebel, Inc.). The decision enabled the reopening of the Distrigas facility in Everett, Massachusetts. The facility received 45 shipments containing 99 Bcf of natural gas in the year 2000, mostly from Trinidad, accounting for nearly half of total LNG imports into the U.S. that year. LNG is an integral part of natural gas supplies for New England, especially during the winter season, when LNG represents around 30% of local distribution company deliveries to consumers.

**Table 1 Sources of LNG Imports for the U.S. in 2001**

Country	U.S. LNG Imports, 2001 (%)
Trinidad	41.2
Algeria	27.3
Nigeria	15.9
Qatar	9.6
Oman	5.1
Australia	1.0



**Figure 2 U.S. LNG Import Facilities**

The Distrigas facility is one of three currently active LNG facilities in the U.S. (Figure 2). The other two active facilities are located in Lake Charles, Louisiana, and Elba Island, Georgia. An additional LNG facility in Cove Point, Maryland, is scheduled to reopen in mid-year 2003. There is growing interest in LNG to supply natural gas for electric power generation and provide supply flexibility. The EIA expects that LNG imports to the U.S. will increase at an average 8.6% per year, that is, to 830 Bcf by 2020.

## **U.S. Environmental Protection Agency (EPA) Risk Management Plans**

The Clean Air Act requires facilities with more than a threshold quantity of a listed extremely hazardous substance to have a risk management program in place and to submit a summary of that program – the Risk Management Plan (RMP) – to the U.S. Environmental Protection Agency (EPA). The List of Regulated Substances includes 77 toxic substances and 63 flammable substances, which can be found in the Code of Federal Regulations (40 CFR 68). Information contained in an RMP for a facility of interest can be helpful in understanding specific facility assets that may be of interest to terrorist groups and the potential consequences of a successful attack.

Among other details, the complete RMP includes a description of (a) the accidental release prevention and emergency response policies at the facility; (b) the facility and the regulated substances handled; (c) the worst-case release scenario(s), defined below, and the alternative release scenario(s), including administrative controls and mitigation measures to limit the distances for each reported scenario; (d) the general accidental release prevention program and chemical-specific prevention steps; (e) the five-year accident history; (f) the emergency response program; and (g) planned changes to improve safety. The owner must include in the worst-case release scenario the off-site consequence analysis (OCA), including the demographics within a certain radius of the facility, as well as environmental receptors within that radius. Executive summaries provided with these documents vary in level of detail but often provide similar detailed information that could be useful to terrorists planning an attack.

Unfortunately, until 1999, the complete RMPs and executive summaries were available publicly and could have been acquired by terrorist organizations. Currently, RMP Executive Summaries cannot be accessed from the EPA directly; however, they can be obtained for most covered facilities from the Right-to-Know Network, located at <http://d1.rtk.net/rmp/wgrmp.php>. Complete RMPs, including the OCA portions, are kept by the EPA. Other governmental agencies may have access to this information upon special request to the EPA.

An estimated 35,000 facilities nationwide, including some large LNG facilities, handle, manufacture, use, or store toxic and flammable substances in quantities above the EPA-regulated thresholds. The worst-case release scenario included in the RMP considers a release of toxic or flammable substances that has the greatest exposure distance in any direction. Some LNG facilities exist near populated areas where a large fire or explosion could threaten a significant population.

Not all LNG facilities have the exact same processes or operate in the same fashion. In addition they do not have similar off-site circumstances. Therefore, an event's consequences will vary for each individual LNG import facility.

An example of a worst-case scenario associated with a release of flammable substances in RMP-covered processes at an LNG import facility might be a vapor cloud explosion, involving the full inventory of the largest storage tank containing LNG. The analysis assumes that the maximum possible inventory is released, completely vaporizes, and ignites, resulting in a vapor-cloud

explosion. If there are public receptor locations just outside the LNG facility, this event could affect members of the public at those closest locations.

## **TERRORIST ACTIVITY INDICATORS**

### **General Characteristics of Terrorist Surveillance**

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 non-mobile 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 will observe a target for a short period of 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 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, global positioning systems, and cellular phones. It should be assumed that many terrorists have access to high-dollar technological equipment.

Electronic surveillance, in this instance, refers to information gathering, legal and illegal, by the terrorists using off-site computers. Such data gathering might include information such as site maps, locations of key facilities, 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 offsite access to the supervisory

control and data acquisition [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 (if feasible) whether attempts are being made to gain access to protected company computer systems and whether any attempts have been successful.

### **Surveillance Indicators**

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 LNG import facility; most of the other indicator categories in this report address activities in a much larger region around the LNG import facility that should be monitored.

### **Other Local and Regional Indicators**

The remaining sets of indicators described in Exhibits 2-5 refer to activities not only in the immediate vicinity of the LNG import facility, but also activities within a relatively large region around the plant (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 there may be several 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 LNG import 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.*

<b>Exhibit 1 Surveillance Indicators Observed Inside or Outside an Installation</b>	
<i>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.</i>	
<b>Persons observed or reported:</b>	
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	Nonmilitary 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.
(Continued on next page.)	



DRAFT – SENSITIVE HOMELAND SECURITY INFORMATION  
LAW ENFORCEMENT SENSITIVE

<b>Activities observed or reported:</b>	
12	A noted pattern or series of false alarms requiring a response by law enforcement or emergency services.
13	Theft of facility or contractor identification cards or uniforms, or unauthorized persons in possession of facility ID cards or uniforms.
14	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.
15	Downloading of materials (e.g., maps, photographs, schematics, or similar materials) that could be used in conjunction with surveillance or attack planning activities.
16	Repeated attempts from the same location or country to access protected computer information systems.
17	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.
18	Attempts to obtain information about the facility (e.g., blueprints of buildings or information from public sources).
19	Unfamiliar cleaning crews or other contract workers with passable credentials; crews or contract workers attempting to access unauthorized areas.
20	A seemingly abandoned or illegally parked vehicle in the area of the facility or asset.
21	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).
22	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.
23	Increase in buildings being left unsecured or doors being left unlocked that are normally locked all the time.
24	Arrest by local police of unknown persons. This would be more important if facility or asset is located in a rural area rather than located in or around a large city.
25	Traces of explosive or radioactive residue on facility vehicles during security checks by detection swipes or devices.
26	Increase in violation of security guard standard operating procedures for staffing key posts.
27	Increase in threats from unidentified sources by telephone, postal mail, or through the e-mail system.
28	Increase in reports of threats from outside known, reliable sources.
29	Sudden losses or theft of guard force communications equipment.
30	Displaced or misaligned manhole covers or other service access doors on or surrounding the facility or asset site.
31	Unusual maintenance activities (e.g., road repairs) near the facility or asset.
32	Observations of unauthorized facility or non-facility personnel collecting or searching through facility trash.

<b>Exhibit 2 Transactional and Behavioral Indicators</b>	
<p><i>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.</i></p>	
<p><b>Transactional Indicators:</b></p> <p>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.</p>	
1	Approach from a previously unknown customer (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 associated with or employed by a military-related business, such as a foreign defense ministry or foreign armed forces.
4	Unusual customer request concerning the shipment or labeling of goods.
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 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 attempts to purchase the exact same product with the same specifications and use, but using a different name.
11	Sale canceled by customer but then the identical product is stolen or “lost” shortly after the customer’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).
13	Customer does not request a performance guarantee, warranty, or service contract where such is typically provided in similar transactions.
(Continued on next page.)	

DRAFT – SENSITIVE HOMELAND SECURITY INFORMATION  
LAW ENFORCEMENT SENSITIVE

<b>Customer Behavioral Indicators:</b>	
What are customer behavioral indicators? Actions or inactions on the part of a customer for equipment or materials that appear to be inconsistent with normal behavioral patterns expected from legitimate commercial customers.	
14	Reluctance to give sufficient explanation of the chemicals or other suspicious materials to be produced with the equipment and/or the purpose or use of those chemicals or materials.
15	Evasive responses.
16	Reluctance to provide information on the locations of the plant 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 usual business or technological level.
20	No request made or declines or refuses the assistance of a 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 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.

<b>Exhibit 3 Weapons Indicators</b>	
<i>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.</i>	
<b>Activities Observed or Reported:</b>	
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 of 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).

DRAFT – SENSITIVE HOMELAND SECURITY INFORMATION  
LAW ENFORCEMENT SENSITIVE

<b>Exhibit 4 Explosive and Incendiary Indicators</b>	
<i>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.</i>	
<b>Persons observed or reported:</b>	
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.
<b>Activities observed or reported:</b>	
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 nonagricultural purchasers or abnormally large amounts to agricultural purchasers.
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 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.

<b>Exhibit 5 Chemical, Biological, and Radiological Indicators</b>	
<i>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.</i>	
<b>Equipment Configuration Indicators:</b>	
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.
<b>Chemical Agent Indicators:</b>	
8	Inappropriate inquiries regarding local chemical sales/storage/transportation points.
9	Purchase or theft of explosives or restricted or sensitive chemicals.
10	Rental of self-storage units and/or delivery of chemicals to such units.
11	Chemical fires, noxious or toxic odors, brightly colored stains, or rusted metal fixtures in apartments, hotel rooms, or self-storage units.
11	Treated or untreated chemical burns or missing hands and/or fingers.
12	Unusual packages or containers, especially near heating, ventilating, and air-conditioning (HVAC) equipment or air intake systems.
13	Unusual powders, droplets, or mist clouds near HVAC equipment or air intake systems.
(Continued on next page.)	

DRAFT – SENSITIVE HOMELAND SECURITY INFORMATION  
LAW ENFORCEMENT SENSITIVE

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

### USEFUL REFERENCE MATERIAL

1. The White House, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, Feb. 2003, available at <http://www.whitehouse.gov/pcipb/physical.html>
2. *Terrorist Attack Indicators*, the html version of the file <http://afsf.lackland.af.mil/Organization/AFSFC/SFP/AF%20Pubs/Terrorist%20Attack%20Indicators.PDF> available at <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 Bulletin, May 15, 2003, available at [http://www.apta.com/services/security/potential\\_indicators.cfm](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*, available at <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*, available at [http://www.globalsecurity.org/intell/library/policy/dod/ct\\_analysis\\_course.htm](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?*, available at <http://web.princeton.edu/sites/publicsafety/>
7. Kentucky State Police: Homeland Security/Counter-Terrorism, *Potential Indicators of WMD Threats or Incidents*, available at <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*, available at [http://www.dtic.mil/afosi/eagle/suspicious\\_behavior.html](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, available at [http://www.homelanddefensejournal.com/archives/pdfs/Feb\\_12\\_vol2\\_iss3.pdf](http://www.homelanddefensejournal.com/archives/pdfs/Feb_12_vol2_iss3.pdf)



10. CH-IV International, *LNG Fact Sheet*, Millersville, MD, available at <http://www.ch-iv.com/lng/lngfact.htm>
11. Sen, Colleen Taylor, *LNG in the Atlantic Basin: Where It Is, Where It's Going*, Gas TIPS, Spring 2002, pp. 24-32, available at [http://www.gastechnology.org/webroot/downloads/en/4ReportsPubs/4\\_7GasTips/Spring02/LNGInTheAtlanticBasin.pdf](http://www.gastechnology.org/webroot/downloads/en/4ReportsPubs/4_7GasTips/Spring02/LNGInTheAtlanticBasin.pdf)
12. Dominion Cove Point LNG, LP, available at <http://www.dom.com/about/gas-transmission/covepoint/index.jsp>
13. U.S. Department of Energy, Energy Information Administration, *Natural Gas Monthly July 2002*, Table 3, p. 6, "Natural Gas Consumption in the United States, 1196-2002," Table 5, p. 10, "U.S. Natural Gas Imports, by Country, 1996–2002."
14. U.S. Department of Energy, Energy Information Administration, *U.S. Natural Gas Markets: Recent Trends and Prospects for the Future*, SR/OIAF/2001-02 (May 2001).
15. U.S. Department of Energy, Energy Information Administration, *United States of America Country Analysis Brief*, accessed 8/22/02 at <http://www.eia.doe.gov/emeu/cabs/usa.html>.
16. Quillen, Doug, *LNG Safety: Myths and Legends*, ChevronTexaco Corp., presented at Natural Gas Technology: Investments in a Healthy U.S. Energy Future, Houston, Texas, May 14-15, 2002, available at <http://www.netl.doe.gov/publications/proceedings/02/ngt/Quillen.pdf>
17. Juckett, Don, *Properties of LNG*, U.S. Department of Energy, LNG Workshop, Solomons, Maryland, February 12, 2002, available at [http://www.fe.doe.gov/oil\\_gas/lngworkshop/index.htm](http://www.fe.doe.gov/oil_gas/lngworkshop/index.htm)
18. How Stuff Works Website, available at <http://science.howstuffworks.com/oil-refining3.htm>
19. U.S. Environmental Protection Agency, *Envirofacts Data Warehouse*, available at <http://www.epa.gov/enviro/>
20. U.S. Environmental Protection Agency, Risk Management Plans, Executive Summaries, available at <http://d1.rtk.net/rmp/wgrmp.php>

### **Related Websites**

1. U.S. Department of Homeland Security, <http://www.dhs.gov/dhspublic/index.jsp>
2. Federal Bureau of Investigation, <http://www.fbi.gov/>
3. American Petroleum Institute, <http://api-ec.api.org/newsplashpage/index.cfm>
4. National Fire Protection Association, <http://www.nfpa.org/>
5. The Right to Know Network, <http://d1.rtk.net>
6. U.S. Department of Commerce, Bureau of Industry and Security, <http://www.bis.doc.gov/>
7. U.S. Environmental Protection Agency, <http://www.epa.gov/epahome/>