POTENTIAL INDICATORS OF TERRORIST ACTIVITY INFRASTRUCTURE CATEGORY: CHEMICAL FACILITIES

Protective Security Division
Department of Homeland Security

Version 2, September 22, 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 the chemical manufacturing industry, which produces and handles large quantities of inherently hazardous materials and manufactures final and intermediate products that are fundamental elements of other economic sectors.

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 chemical plant 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.

CHEMICAL MANUFACTURING INDUSTRY BACKGROUND

Terrorists Targeting Objectives

To consider terrorist threat indicators in relationship to the chemical manufacturing industry, it is useful to understand the basic structure of the industry and what general types of facilities might be attractive targets for terrorist attack. Chemical manufacturing facilities are attractive terrorist targets because many of the chemical agents stored, processed, and transported to and from chemical manufacturing facilities could be used as weapons of mass destruction (WMD). Generally speaking, terrorists or terrorist groups may target chemical manufacturing facilities to either (1) sabotage the facility or (2) divert chemicals or other materials for other purposes, as depicted in Figure 1.

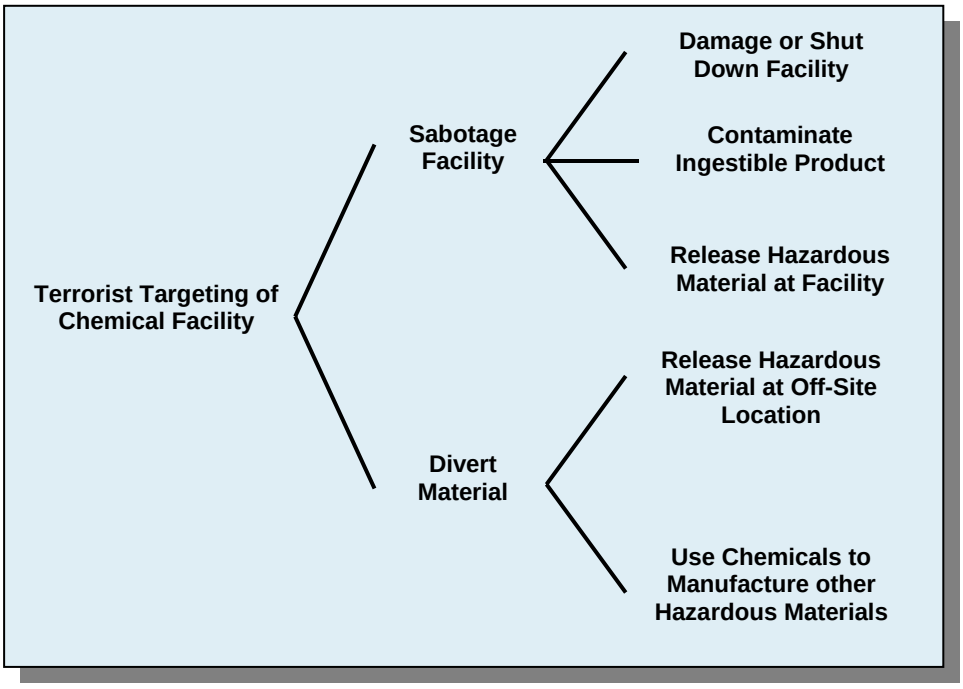

Figure 1 Terrorist Targeting Objectives for Chemical Manufacturing Facilities

Facility sabotage can be intended to (1) damage the facility and cause economic, national security, or logistical harm; (2) contaminate product going into the food, medical, or health care system; or (3) "weaponize" the facility against the surrounding human population by causing the release of hazardous materials from the plant site. Material diversion would most likely be for weaponization purposes to cause bodily harm or death, but not necessarily in the vicinity of the facility. Diverted chemical materials or equipment might be used in their original form or for manufacturing other toxic, hazardous, explosive, or incendiary substances.

Sector Description

The United States (U.S.) chemical manufacturing industry produces approximately 15,000 commercial chemicals in large quantities. The largest three segments of the industry are organic, inorganic, and agricultural chemicals. Table 1 highlights the typical plant size and regional concentrations found in each segment. Although many facilities are small, those that are large are typically very large and contain many integrated processes.

Organic and inorganic chemicals industries obtain raw materials from petroleum and mined products, respectively, and convert them to intermediate materials or basic finished chemicals. Organic, or carbon-containing, chemicals account for most of the large-quantity commercial chemicals. This class of chemicals is of interest to terrorists because it includes many of the toxic and hazardous chemicals that are precursors to, or can be used directly as, chemical weapons. A subclass of inorganic chemicals known as chlor-alkali includes chlorine and caustic soda, which may be of interest to terrorists because of the hazardous nature of these materials and the damaging health effects that chlorine can cause if inhaled. Finally, agricultural chemicals are attractive to terrorists because this group includes herbicides and pesticides, which can form the basis for chemical weapons, and nitrogenous fertilizers, which have frequently been used as improvised explosive devices (e.g., ammonium nitrate mixed with fuel oil).

Table 1 Demographics of Major Chemical Manufacturing Industry Segments

Major Segment	Typical Facility Size	Regional Concentration	
		Sub-Segment	Region
Organic	Small (70% < 100 Employees)	• Gum and Wood-Based • Petroleum-Based	• Southeast • Gulf Coast, Northeast, Midwest
Inorganic	Small (80% < 50 Employees)	• Chlor-Alkali • Others	• Gulf Coast, Great Lakes Region, Southeast, Northwest • Gulf Coast, Great Lakes Region
Agricultural	Pesticides – Small Others – Large	• Pesticides • Ammonia • Nitric Acid • Phosphoric Acid	• Midwest, Great Plains, Gulf Coast • Louisiana, Texas, Oklahoma, Iowa, Nebraska • Midwest, South Central, Gulf Coast • Florida, Southeast

Chemical Materials That Could Be Used in Terrorist Activities

The Federal Bureau of Investigation (FBI) is working with other federal agencies to assess the chemical and biological materials that may be used in furtherance of WMD terrorism. The FBI put together Table 2, based on available public source materials, FBI investigations, product availability, and the evaluation of complex manufacturing and development processes. The FBI continually updates this list, and therefore, it should not be viewed as a final and absolute list of potential WMD chemicals. It is important, however, to consider these and subsequent potential WMD chemicals identified by the FBI when evaluating evidence of plant surveillance, suspicious activities, or other indicators of terrorist activity in relation to chemical manufacturing facilities.

Additional sensitive chemicals and chemical precursors are identified as part of the Chemical Weapons Convention (CWC). The U.S. is one of more than 151 State parties to the CWC, which prohibits the development, production, stockpiling, and use of chemical weapons. The CWC does not prohibit production, processing, consumption, or trade of related chemicals for peaceful purposes, but it does establish a verification regime to ensure such activities are consistent with the object and purpose of the treaty.

Table 2 Chemicals That Could Be Used in Terrorist Activities

Ammonia*	Arsenic	Arsine
Boron trichloride	Boron trifluoride	Butyric acid
Carbon disulfide	Chlorine*	Chloroacetone
Cyanides*	Diborane	Dimethyl sulfate
Dimethyl sulfoxide	Ethylene oxide	Fluorine
Formaldehyde	Hydrogen bromide	Hydrogen chloride**
Hydrogen fluoride	Hydrogen sulfide	Mercury
Methyl phosphonothioic	Dichloride	Methyl phosphonous dichloride
Methyl phosphonyl dichloride	Methyl phosphonyl difluoride	N,N'-Dicyclohexylcarbo-diimide
N,N'-Diisopropylcarbo-diimide	N,N'-Dimethylamino	Phosphoryl dichloride
Nitric acid	Phosphine	Phosphorus trichloride
Sodium azide	Sodium fluoroacetate	Sulfur dioxide
Sulfuric acid**	Thallium	Thiodiglycol
Thionyl chloride	Tributylamine	Tungsten hexafluoride
2-(Diisopropylamino) ethane thiol	2-(Diisopropylamino) ethanol	

* Chemical agents that are more likely to be used in furtherance of WMD terrorism or criminal activity.
** Interest in these chemicals depends on the concentration and whether it is in the anhydrous form.

Toxic chemicals and chemical precursors[1] under purview of the CWC are classified in three categories, depending on the historic use of the chemical as a weapon, the capability of the chemical to be used as a weapon, the toxicity of the chemical, and quantities produced for legitimate commercial purposes. The categories include the following:

[1] Precursor chemicals are typically those chemicals that require only one additional reaction stage to produce a designated toxic chemical or an important constituent of a designated toxic chemical.

Schedule 1 Military Agents with No or Low Commercial Use,
Schedule 2 Precursors and Toxic Chemicals with Moderate Commercial Use,
Schedule 3 High Commercial Volume Dual-Use Chemicals.

The list of chemicals classified under each CWC category can be found in Reference 16.

In addition, the Australia Group [http://www.australiagroup.net] has developed lists of chemical weapons precursors, dual-use chemical manufacturing facilities and related technology, dual-use biological equipment, biological agents, and plant and animal pathogens that could be used in the proliferation of chemical and biological weapons. The Australia Group aims to ensure that exports of these items from the group's countries do not contribute to the spread of chemical and biological weapons (CBW) without impeding trade of materials and equipment used for legitimate commercial purposes. The group works towards this goal by licensing certain chemicals, biological agents, and dual-use chemical and biological manufacturing equipment. All states participating in the Australia Group, including the U.S., are parties to the Chemical Weapons Convention (CWC) and the Biological Weapons Convention (BWC).

Environmental Protection Agency (EPA) Risk Management Plans

All chemical facilities that use or produce chemicals are required to have a Material Safety Data Sheet (MSDS) for each chemical. They have also developed emergency response plans in collaboration with local fire and other first responders under the requirements of the Emergency Planning and Community Right to Know Act (EPCRA). The chemical lists are given to the local emergency planning committee, the state emergency response committee, and the local fire department. Again, the facility emergency response plans may be a useful source of information regarding potential target chemicals plans in place to prevent and mitigate a release.

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 Risk Management Plan (RMP) to the 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—including any chemical plant using, storing, manufacturing, or handling toxic or flammable chemicals—can be helpful in understanding the specific facility assets that might be of interest to terrorist groups and the potential consequences of a successful attack.

Unfortunately, until 1999, the executive summaries were available publicly and could have been acquired by terrorist organizations. Currently, RMP executive summaries can no longer be accessed from the EPA website directly. The EPA keeps complete RMPs, including the off-site consequence analysis (OCA), which describes the demographics within a certain radius of the facility as well as environmental receptors within that radius. Other governmental agencies may have access to this information upon special request to the EPA. In addition, complete RMPs and OCA information are available (with certain restrictions) for viewing in paper form at EPA and Department of Justice (DOJ) Reading Rooms located throughout the U.S. Such access is required by Public Law 106-40 (the Chemical Safety Information, Site Security, and Fuels

Regulatory Relief Act, Ref. 20). However, RMP information can be obtained for most covered facilities from the Right-to-Know Network [http://d1.rtk.net/rmp/wgrmp.php]. This website could be an important source of information for terrorists to use in selecting targets and estimating the consequences of their attack scenarios.

The executive summaries available on the Internet vary in level of detail but often provide information that could be useful to terrorists planning an attack. These summaries must, by regulation, include a description of (1) the accidental release prevention and emergency response policies at the facility; (2) the facility and the regulated substances handled; (3) 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; (4) the general accidental release prevention program and chemical-specific prevention steps; (5) the five-year accident history; (6) the emergency response program; and (7) planned changes to improve safety. Some executive summaries also contain detailed OCA information.

An estimated 15,000 facilities nationwide 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 hypothetical release of toxic or flammable substances that has the greatest exposure distance in any direction. Many facilities exist in populated areas where a chemical release could threaten thousands. The EPA reports that 123 chemical facilities located throughout the nation have worst-case scenarios in which more than one million people are within the circle whose radius is equal to the “endpoint distance” of the hypothetical vapor cloud (“vulnerable zone”). Since toxic vapor generally travels only in the downwind direction, only people located under the plume within the vulnerable zone could actually be exposed. Each of about 586 facilities has a vulnerable zone with between 100,001 and 1 million people. Each of about 2,000 facilities has a vulnerable zone with between 10,001 and 100,000 people.

The chemicals stored, used, and manufactured obviously vary with each type of chemical plant. However, a common example of a worst-case scenario associated with a hazardous chemical release in RMP-covered processes at a chemical facility might be a catastrophic failure of a chlorine railroad tank car, which could produce a chlorine plume that could travel more than 25 miles before dispersing enough to no longer pose a public hazard. If public receptor locations exist just outside the chemical facility’s property, this event could affect members of the public at the closest locations. RMP worst-case scenarios are based on the assumption that the release is accidental. Therefore, an act of malfeasance may produce different results than those contemplated under an RMP. However, RMP executive summaries may provide terrorists with a valuable source of information on potential target chemicals and consequences, as well as steps the facility has taken to prevent a release.

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 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 high-dollar 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 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 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 chemical plant; 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 chemical plant, 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 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 chemical plant 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	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	Nonfacility 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 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 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 nonfacility 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 (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. (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 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 WMD).
13	Customer does not request a performance guarantee, warranty, or service contract where such is typically provided in similar transactions.
	Continued on next page.

Customer Behavioral Indicators *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 plant 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 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.
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, chemical processes, packaging configurations, or other indicators to suggest this person may not be routinely involved in purchasing chemicals.
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 nonagricultural 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 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 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, 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.
	Continued on next page.

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.
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 nonagricultural 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 heating, ventilating, and air-conditioning (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.
31	Large number of unexplained human or animal deaths.
33	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 [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 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. Environmental Protection Agency, *Envirofacts Data Warehouse* [http://www.epa.gov/enviro/]. This site has information about EPA-regulated chemical

facilities. For example, users can obtain maps showing the facility and lists of toxic chemicals used or produced at the site.

11. Risk management plans and executive summaries formerly available from the U.S. Environmental Protection Agency are currently available from the Right-to-Know Network [http://d1.rtk.net/rmp/wgrmp.php]. This site has information listed by state for all chemical plants that have filed risk management plans. The executive summary includes a description of the worst-case release scenario for regulated toxic chemicals and regulated flammable chemicals.

12. U.S. General Accounting Office, *Homeland Security: Voluntary Initiatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness is Unknown*, GAO-03-439, March 2003 [http://www.gao.gov/].

13. American Chemistry Council, Chlorine Institute, Synthetic Organic Chemical Manufacturers Association, *Site Security Guidelines for the U.S. Chemical Industry*, Oct. 2001 [http://www.americanchemistry.com/].

14. American Institute of Chemical Engineers, *Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites*, Center for Chemical Process Safety, Aug. 2002 [http://www.aiche.org/ccpssecurity/].

15. Tour, James M., "Do-It-Yourself Chemical Weapons," *Chemical & Engineering News*, Vol. 78, No. 28, pp. 42–45 [http://pubs.acs.org/hotartcl/cenear/000710/7828perspective.html].

16. U.S. Chemical Weapons Convention Web Site, Annex on Chemicals [http://www.cwc.gov/treaty/annex_chem/annonchem_html#Sched-B]. This web site lists chemicals that are considered toxic or as weapons precursors.

17. Belke, James C., *Chemical Accident Risks in U.S. Industry — A Preliminary Analysis of Accident Risk Data from U.S. Hazardous Chemical Facilities*, U.S. Environmental Protection Agency, Chemical Emergency Preparedness and Prevention Office, Washington, D.C., Sept. 25, 2000. This paper contains an analysis of information provided in the chemical industry risk management plans covering the 1994–1999 time period.

18. U.S. Environmental Protection Agency, Chemical Emergency Preparedness and Prevention Office, *Consolidated List of Chemicals Subject to Emergency Planning and Community Right-to-Know Act (EPCRA) and Section 112(r) of the Clean Air Act*, EPA-550-B-01-03, Oct. 2001 [http://yosemite.epa.gov/oswer/ceppoweb.nsf/vwResourcesByFilename/title3.pdf/$file/title3.pdf].

19. National Fire Protection Association, Hazard Ratings under NFPA 704—Standard System for the Identification of the Hazards of Materials for Emergency Response

[http://www.unomaha.edu/~wwwehs/NFPA704/nfpa_704_ratings_for_common_chem.htm].

20. U.S. Environmental Protection Agency, Chemical Emergency Preparedness and Prevention Office, EPA Federal Reading Rooms [http://yosemite.epa.gov/oswer/ceppoweb.nsf/content/readingroom.htm].

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. Agency for Toxic Substances and Disease Registry [http://www.atsdr.cdc.gov/].
4. American Chemistry Council [http://www.americanchemistry.com/].
5. American Chemistry Society [http://www.chemistry.org/portal/a/c/s/1/home.html].
6. American Institute of Chemical Engineers [http://www.aiche.org/].
7. American Petroleum Institute [http://api-ec.api.org/newsplashpage/index.cfm].
8. Center for Chemical Process Safety [http://www.aiche.org/ccps/].
9. Centers for Disease Control and Prevention [http://www.cdc.gov/].
10. Chlorine Institute, Inc. [http://www.cl2.com/].
11. National Association of Chemical Distributors [http://www.nacd.com/index.cfm].
12. National Fire Protection Association [http://www.nfpa.org/].
13. The Right to Know Network [http://d1.rtk.net].
14. Synthetic Organic Chemical Manufacturers Association [http://www.socma.com/].
15. U.S. Chemical Weapons Convention Web Site [http://www.cwc.gov/].
16. U.S. Department of Commerce, Bureau of Industry and Security [http://www.bis.doc.gov/].
17. U.S. Environmental Protection Agency [http://www.epa.gov/epahome/].