POTENTIAL INDICATORS OF TERRORIST ACTIVITY INFRASTRUCTURE CATEGORY: CHEMICAL STORAGE FACILITIES

Protective Security Division
Department of Homeland Security

Draft Version 1, January 30, 2004

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 chemical storage facilities.

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 STORAGE FACILITY BACKGROUND

Terrorists Targeting Objectives

To consider terrorist threat indicators in relationship to chemical storage 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. Chemical storage facilities are attractive terrorist targets because they can contain toxic and hazardous materials, can create extensive casualties and property damage, and can be a source of materials for use in other attacks. Figure 1 shows some of the potential terrorist targeting objectives.

Damage or destruction of the facility can be intended to inflict casualties, both on- and offsite, shut down or degrade the operation of the facility, or 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 them to other uses or to reap financial gain from their resale. Theft of information can be intended to acquire insight that is not made public or to gain data that can be used in carrying out attacks. Facility attacks can be intended to (1) 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.

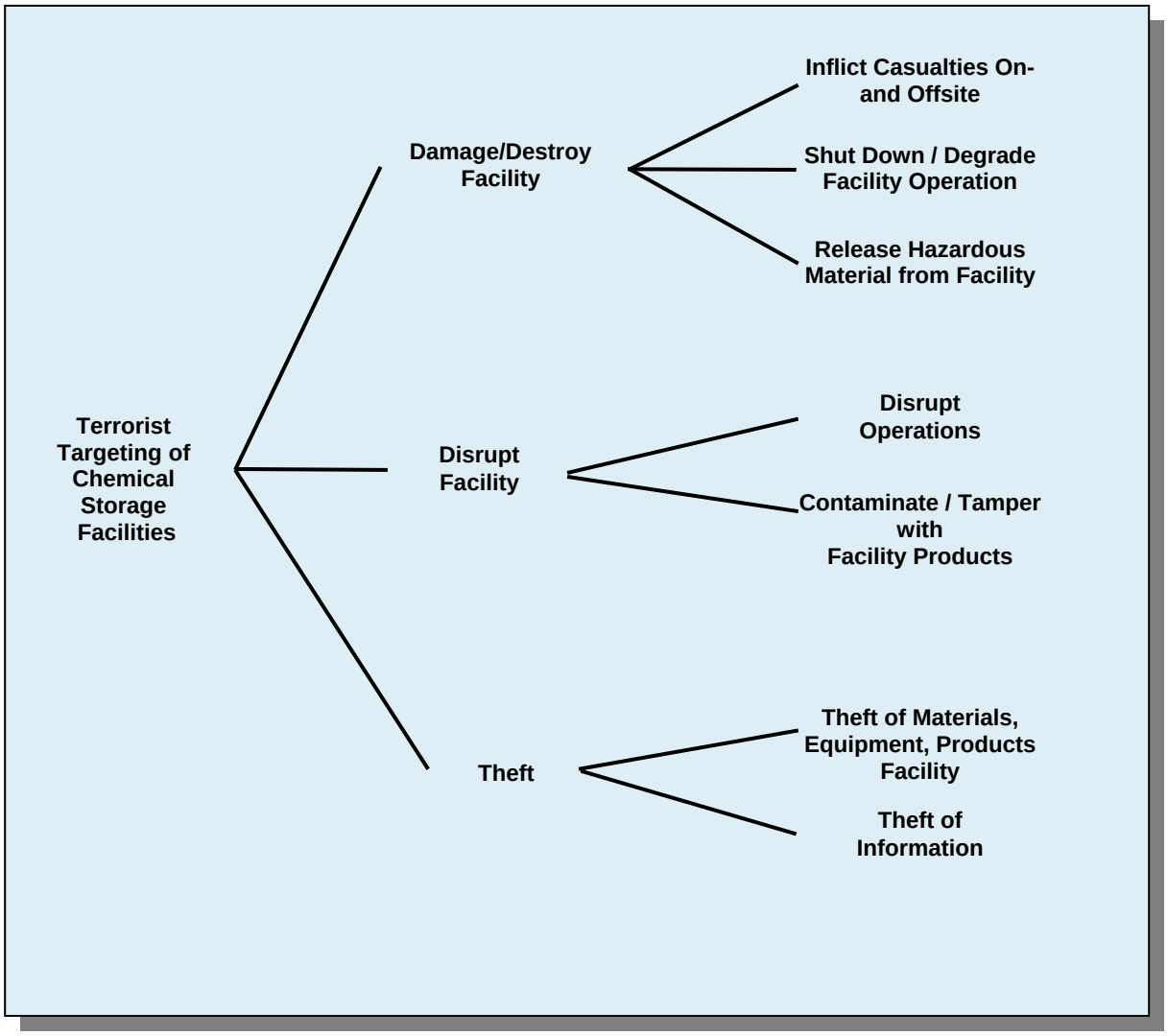

Figure 1 Terrorist Targeting Objectives

Sector Description

The chemical manufacturing industry produces an enormous number of materials. Government sources estimate that 15,000 chemicals are manufactured in the United States (U.S.) in quantities greater than 10,000 pounds (U.S. Environmental Protection Agency [EPA] 2002). The organic chemicals industry, which manufactures carbon-containing chemicals, accounts for much of this diversity.

The North American Industry Classification System (NAICS) was developed by the statistical agencies of Canada, Mexico, and the U.S. to provide common definitions of the industries within the three countries and a common statistical framework for analyzing statistical data relating to industry and the economy. It has a hierarchical structure, dividing the economy into 20 sectors at its highest level. The general structure of the chemical storage industry by NAICS codes is shown in Table 1. The "Other Chemical & Allied Product Wholesaler" sector handles a variety of toxic and flammable compounds as raw materials, intermediates, or finished products. The other two sectors in Table 1 handle either quantities of agricultural chemicals (NAICS 42291) or incidental amounts of toxic or flammable materials (NAICS 4931).

Table 1 Structure of the Chemical Storage Industry

NAICS Code	Industry Sector
42269	Other Chemical & Allied Product Wholesalers
42291	Farm Suppliers Wholesalers
4931	Warehousing & Storage

Approximately $18 billion of U.S. chemical industry sales are made through chemical distributors, who are also actively engaged in various phases of import/export trade that contributes significantly to the total chemical industry's annual positive balance of trade. Companies are largely entrepreneurial and generally service a particular geographic region and specific industrial sector. The distributors' industrial customers use these materials to produce an endless list of products, including food flavorings, perfumes, water purifiers, computers, plastics, paints and coatings, textiles, cosmetics and toiletries, detergents, automobile parts, rubber compounds, fiberglass, pharmaceuticals, and many other products.

Chemical storage facilities are among the most common areas containing either toxic or flammable compounds with quantities sufficient to require the facility to submit a Risk Management Plan (RMP) to the EPA. As shown in Table 2, farm suppliers' wholesalers are the most prevalent facility handling either toxic or hazardous materials. The most prevalent toxic chemical processes, including refrigeration systems and fertilizer storage containers, generally contain relatively small chemical quantities.

Table 2 Number of RMP Processes for the Chemical Storage Sector

NAICS Code	Industry Sector	Rank	No. of Processes
42269	Other Chemical & Allied Product Wholesalers	6th	607
42291	Farm Suppliers' Wholesalers	1st	4,409
49311	General Warehousing & Storage Facilities	20th	151
49312	Refrigerated Warehousing & Storage Facilities	7th	549
49313	Farm Product Warehousing & Storage Facilities	11th	345

Four chemicals—anhydrous ammonia, chlorine, propane, and flammable mixtures—are present in nearly 70% of all RMP processes. Anhydrous ammonia is predominant because of its several widespread uses, including fertilizer production, refrigeration, and land application as an agricultural nutrient. It alone is present in about one-third of all RMP chemical processes and 48% of all toxic chemical processes. The high number of chlorine processes is mainly due to the common use of chlorine for disinfecting water.

Other Chemical and Allied Product Wholesalers. This U.S. industry segment comprises establishments primarily engaged in wholesaling chemicals and allied products (except agricultural and medicinal chemicals, paints and varnishes, fireworks, plastics materials, and basic forms and shapes). The U.S. has a total of 11,571 facilities, of which 1,106 handle and store industrial gases and 10,465 handle and store chemicals and allied products (Commerce 1997).

More than 50% of U.S. chemical wholesaling facilities are located in eight states: California, Florida, Georgia, Illinois, New Jersey, New York, Ohio, and Texas. It seems that the number of chemical wholesaling facilities roughly tracks with state population, with states with larger populations having a greater number of establishments.

Farm Suppliers Wholesalers. This U.S. industry segment comprises establishments primarily engaged in wholesaling farm supplies, such as animal feeds, fertilizers, agricultural chemicals, pesticides, plant seeds, and plant bulbs. The U.S. has a total of 7,378 farm suppliers' facilities, of which 3,873 are farm dealers and 3,505 are wholesale distributors (Commerce 1997).

Many of these establishments are small and have another primary line of business other than storing and distributing pesticides and other miscellaneous agricultural chemicals. Because the Census Bureau only counts those facilities that report an NAICS code as their primary line of business, the number of facilities identified above is not inclusive of all facilities involved in agricultural chemical storage.

More than 50% of U.S. farm suppliers wholesaling facilities are located in 10 states: California, Texas, Illinois, Iowa, Florida, Missouri, Minnesota, New York, Indiana, and Ohio. The majority of farm suppliers wholesalers are located in agricultural regions, such as the Midwest, South

Central, and Gulf States, to accommodate the high volume of fertilizer usage. Florida has the largest phosphate rock supply in the U.S.; thus, phosphoric acid manufacturing is concentrated primarily in Florida and spreads into the Southeast.

Warehousing and Storage. The warehousing and storage industry segment is classified by NAICS Group 4931. Industry Group 4931 includes these NAICS codes:

49311 – General Warehousing & Storage,

49312 – Refrigerated Warehousing & Storage Facilities,

49313 – Farm Product Warehousing & Storage Facilities, and

49319 – Other Warehousing & Storage Facilities.

The General Warehousing & Storage sector comprises establishments primarily engaged in operating merchandise warehousing and storage facilities. These establishments generally handle goods in containers, such as boxes, barrels, and drums, using equipment, such as forklifts, pallets, and racks. These facilities typically store commodities other than hazardous or flammable chemicals. However, materials at risk at these facilities include butane and flammable mixtures (for aerosol cans).

Anhydrous ammonia may be present at refrigerated warehousing and storage facilities, farm product warehousing and storage facilities, and other warehousing and storage facilities (Indiana Department of Environmental Management). The quantities of hazardous and flammable materials in storage at these facilities are typically much lower than at chemical wholesalers.

More than 50% of U.S. warehouse and storage facilities are located in nine states: California, Texas, New Jersey, New York, Florida, Illinois, Ohio, Georgia, and Pennsylvania. It seems that the number of warehouse and storage facilities roughly tracks with state population; that is, states with larger populations have a greater number of establishments.

Common Facility Characteristics. Storage is a means of holding and preserving products from the time of production until the final use. Storage forms an essential support facility in the production and distribution process. The availability of storage facilities at all levels ensures a steady flow of raw materials, spare parts, and consumer goods and has a strong influence on the prices paid by the final consumer.

Chemical distribution facilities are involved in the warehousing, storage, and refrigeration of products, such as acids, industrial and heavy chemicals, dyestuffs, industrial salts, rosins, and turpentines. These facilities may also be engaged in the formulation and repackaging of bulk or packaged materials to be transferred offsite. In addition, chemical distribution facilities may perform plant maintenance activities and wastewater treatment.

A chemical distribution facility consists of upstream components, process units, downstream components, and product storage. Chemical storage activities can be further divided into the following stages, each of which may contain one or more activities: (1) the chemical products are coming in; (2) the chemicals are temporarily stored awaiting shipment; and (3) the chemical

product is being shipped out. One way to determine which activities provide a potential for a disruption event is to review the following attributes for each activity:

- The type of process equipment, including storage vessels, and activities, such as loading, that involves a regulated substance and could lead to an accidental release;
- The specific chemicals being used or produced and whether or not they are listed in 40 CFR 68.130, 29 CFR 1910.119, 49 CFR 172.101 ("hazardous materials" for the purpose of transportation), 33 CFR 126, 127, 154; or chemicals governed by the Chemical Weapons Convention, identified by the Federal Bureau of Investigation (FBI) as "chemicals for potential misuse as weapons of mass destruction" (FBI-List chemicals), or those identified by the Australia Group[1] [http://www.australiagroup.net/];
- The quantity, form, and concentration of the chemicals;
- The accessibility and recognizability of the chemicals; and
- The potential for theft, product contamination, or offsite release of the chemicals.

Transportation containers that have been unhooked from the motive power that delivered them to the site (e.g., truck or locomotive) and left on a site for short- or long-term storage may also be considered a chemical storage facility. A tank truck that is being unloaded with the motive power still attached may be considered to be in transport and is not considered in this analysis.

Warehouses that handle or store chemicals usually consist of one large storage area, even if subdivided, and are likely to have the same prevention practices for the entire warehouse. Some of these warehouses may repackage chemicals, but most limit their activities to storing substances in containers designed to meet U.S. Department of Transportation (DOT) transportation regulations.

Chemical storage facilities differ according to their complexity and physical configuration. Nevertheless, Figure 2 provides an example of the typical process flow for a chemical storage facility. Figure 3 is a photo of an actual chemical storage facility.

[1] The Australia Group of countries aims to ensure through licensing of certain chemicals, biological agents, and dual-use chemical and biological manufacturing equipment, that exports of these items from their 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. All states participating in the Australia Group, including the United States, are parties to the Chemical Weapons Convention (CWC) and the Biological Weapons Convention (BWC).

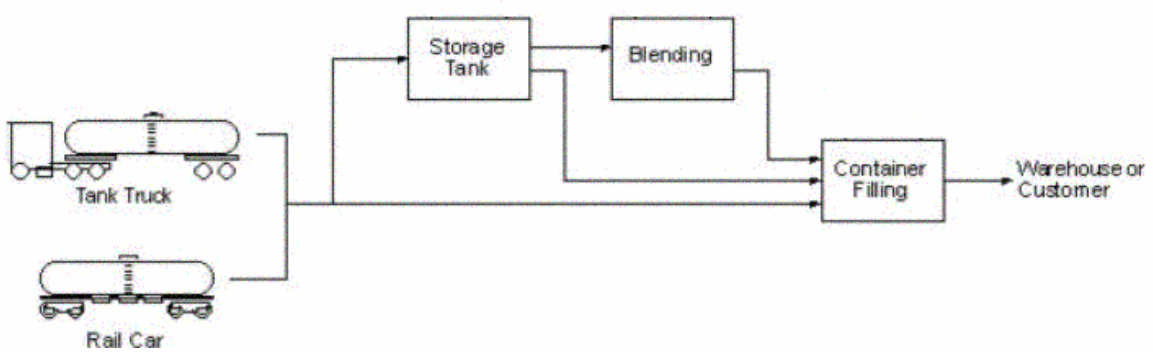

Figure 2 Chemical Storage Facility Process Flow
[http://www.ncjrs.org/pdffiles1/nij/195171.pdf]

Figure 3 Chemical Storage Facility
[http://www.sntg.com/]

The industry has identified three categories of potential consequences of a successful attack on a facility:

1. Uncontrolled release of material,
2. Theft of material, and
3. Contamination of product or process.

For uncontrolled release of material, the severity of the consequences would depend on (1) the toxicity of the material on the site, (2) the amount of material, (3) the actions of the material if released, (4) the accessibility of the material to attack, (5) the ability of the facility and community to respond, free from interdiction.

Consequences of the theft of material is a function of (1) the attractiveness of the material as a weapon; (2) the attractiveness of the material as a means to make a weapon; (3) the way in which the material is stored or shipped (small, portable units versus large containers); (4) the accessibility of the material to theft; and (5) the chemistry involved in making a deliverable weapon out of the material in question.

Product contamination comes in two forms. First, and most obvious, is the introduction of a tainting agent into a chemical that will find its way into public use. The classic example is the addition of cyanide to several bottles of Tylenol. Such sabotage at the root chemical level could have far-ranging consequences, depending on the post-sabotage processing.

TERRORIST ACTIVITY INDICATORS

There are several indicators of possible terrorist activity that should be monitored on a regular basis. Constant attention to these indicators can help to 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 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 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 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 offsite computers. This type of data gathering might include obtaining 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 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 offsite 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.

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 2–5 refer to activities not only in the immediate vicinity of the facility, but also activities within a relatively large region around the plant (e.g., 100 to 200 miles). While local authorities should be aware of such activities, they 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 offsite 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 offsite 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 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 (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 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.)

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 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 onsite or offsite 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.
	(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 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 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.
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

1. White House, *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 surveillance, 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. Agricultural Retailers Association, *Guidelines to Help Ensure a Secure Agribusiness* [http://www.aradc.org/secureagribusinessguidelines.pdf].

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

12. ACC website [http://www.americanchemistry.com].

13. ACC Responsible Care website [http://www.responsiblecaretoolkit.com/security.asp].

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. ATSDR Report on Chemical Terrorism, *Industrial Chemicals and Terrorism: Human Health Threat Analysis, Mitigation and Prevention* [http://www.mapcruzin.com/scruztri/docs/cep1118992.htm].

16. Baybutt, Paul, and Varik 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].

17. Belke, J.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, DC, Sept. 25, 2000. This paper contains analysis of information provided in the chemical industry risk management plans covering the 1994–1999 time period. [http://www.epa.gov/ceppo/pubs/stockholmpaper.pdf].

18. Chemical Alliance, *Chemical Accident Prevention: Site Security* [http://www.chemalliance.org/docs/SECALE-F.PDF].

19. Dangerous Goods Advisory Council, *Security Talking Points* [http://www.hmac.org/miscellaneous/security.htm].

20. Indiana Department of Environmental Management, Office of Air Quality, "Summary of Risk Management Plans for Indiana Sources Using RMP Info" [http://www.state.in.us/idem/air/programs/112r/screenweb.pdf].

21. National Association of Chemical Distributors, *The Responsible Distribution Process*^{SM}, *Code of Management Practice* [http://www.nacd.com/Rdp/RDP_CMP.pdf].

22. 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].

23. North Carolina Department of Agriculture and Consumer Services, *Terrorism Threat Vulnerability Self Assessment Tool* [http://www.ncagr.com/industry_self-assessment.doc].

24. Tour, J.M., "Do-It-Yourself Chemical Weapons," *Chemical & Engineering News*, 78(28):42-45 [http://pubs.acs.org/hotartcl/cenear/000710/7828perspective.html].

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

26. 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.

27. 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.

28. U.S. Environmental Protection Agency, Risk Management Plans, Executive Summaries [http://d1.rtk.net/rmp/wgrmp.php]. This site has information listed by state for all chemical facilities 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.

29. 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].

30. 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.

31. 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/].

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

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