POTENTIAL INDICATORS OF TERRORIST ACTIVITY INFRASTRUCTURE CATEGORY: AGRICULTURAL STORAGE FACILITIES

Protective Security Division
Department of Homeland Security

DRAFT - Version 1.0, December 15, 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 agricultural storage facilities, which hold large quantities of raw agricultural products and supplies, house live animals at rearing and slaughtering facilities, or store processed foods prior to transport of and distribution to retail sales locations and restaurants.

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 agricultural storage facility of interest and what it might look like. The key factor to early recognition of terrorist activity is the ability to recognize anomalies in location, timing, and character of vehicles, equipment, people, and packages.

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

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

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

In some cases, the terrorists' 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 for 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.

AGRICULTURAL STORAGE FACILITIES BACKGROUND

Terrorist Targeting Objectives

To consider terrorist threat indicators in relationship to agricultural storage facilities, it is useful to understand the characteristics of those facilities and why they might be attractive targets for terrorist attack.

Two types of "anti-agricultural" biological weapons have been developed: (1) weapons that are lethal to humans but do not spread easily from one person to another and (2) weapons that target crops and livestock with contagions that are highly communicable among their non-human hosts. The latter type of weapon may be more attractive to terrorists because widespread contagions could result from a small infectious initiating event of crops or livestock.

Once a terrorist group obtains an agricultural biological weapon, it must be disseminated widely enough to cause significant damage to the industry. Terrorists or terrorist groups may target agricultural storage facilities to (1) cause illness or death and/or (2) cause fear and serious economic harm, as depicted in Figure 1. Contaminating the food supply could cause illness or death. Fear and serious economic harm, as well as an erosion in public confidence in the food supply, could lead to panic buying, hoarding, and possibly severe shortages of foodstuffs. Loss of crops or livestock would have a direct economic effect on the United States (U.S.) agricultural industry, from farm to table, as well as a long-term impact on the commodities markets.
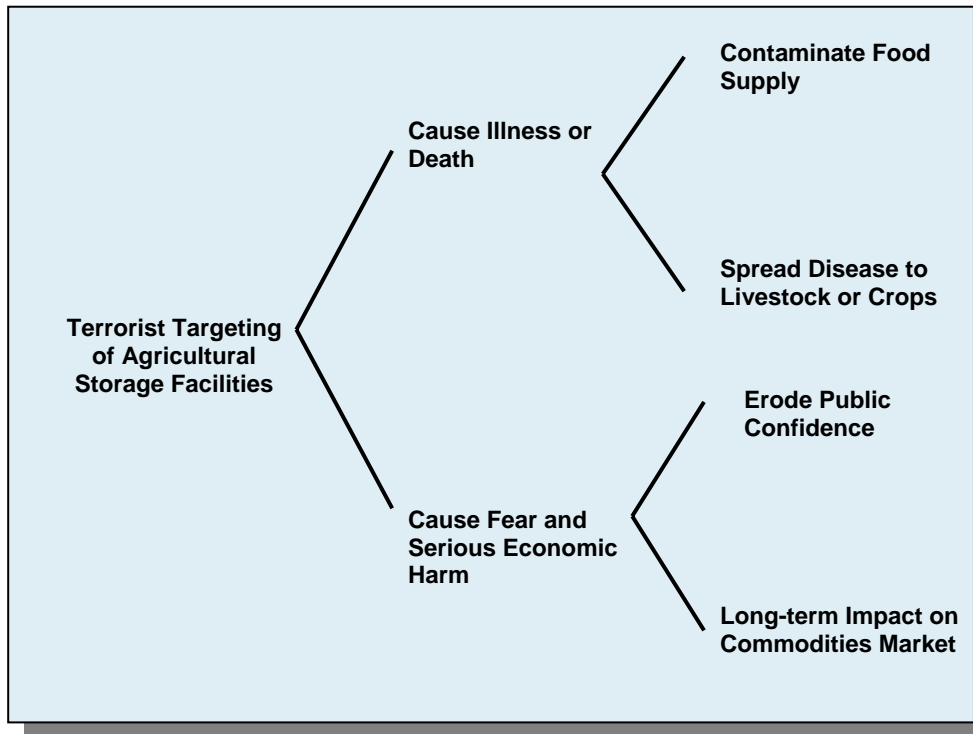
Figure 1 Terrorist Targeting Objectives for Agricultural Storage Facilities

Sector Description

Traditionally, food in America is produced through a series of processes commonly referred to as the "farm-to-table" continuum (see Figure 2). This process is comprised of multiple components, including production, distribution, processing, transportation, wholesaling, exporting and importing, retail sales, and consumption. Each component of the farm-to-table continuum is achieved in various ways specific to the end product being produced. At multiple stages of these processes, raw agricultural products, farm input supplies, and consumer-ready foods are stored in large facilities. These facilities store raw agricultural products (wheat, corn, apples) prior to processing; farm input supplies (fertilizers, seed, chemicals); live animals (cattle, swine, chickens); or processed products ready for distribution and consumption (cheese, cereals, packaged products). In this regard, there is not a "typical" agricultural storage facility. Rather, various facilities specific to the storage requirements of a given product or component serve the farm-to-table continuum.
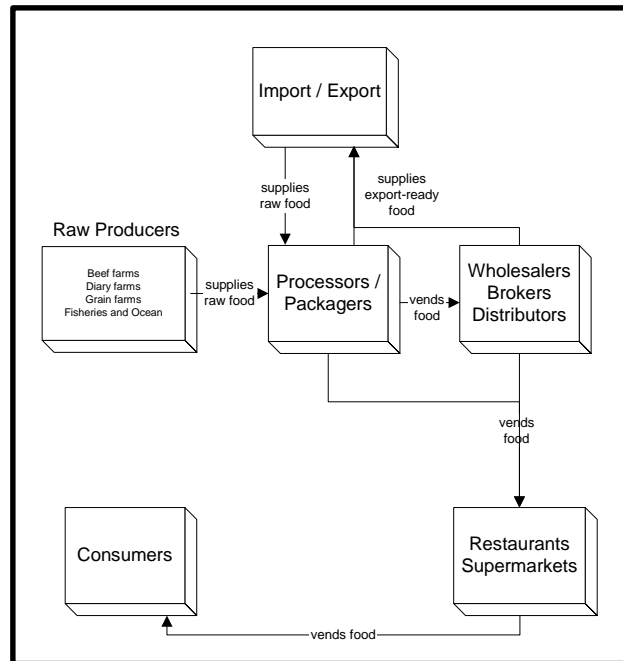
Figure 2 Farm-to-Table Continuum

Across the stated continuum, agricultural storage facilities are quite varied.

- Raw agricultural products are stored in facilities designed to receive and house
  a variety of goods from local producers. Figure 3 shows an "on-farm" grain storage
  facility. Local producers send their products to storage facilities at processing plants
  or facilities that store raw agricultural products before they are distributed to
  processing facilities. Traditionally, these facilities are located near rural farming
  communities from which their particular products are grown.

- Animal and aquaculture slaughtering and rearing facilities are another aspect of
  agricultural storage. These facilities have unique vulnerabilities. Due to efficiencies
  gained in animal production as well as storage and distribution, specific
  vulnerabilities surround the dissemination of transmittable diseases and the rapid
  distribution of contaminated products across the country. Currently, just 2% of
  America's feedlots produce 78% of U.S. cattle (see Figure 4 for an example of a
  feedlot). Nearly all cattle are processed in four slaughterhouses, and almost all hogs
  move through four separate slaughterhouses. Nine farms produce 59% of the
  country's broiler chickens. Poultry, swine, and beef storage, slaughtering, and
  distribution efforts are regionally based, and as such, the storage facilities associated
  with each commodity are regionally located. This particular "storage" vulnerability
  has massive economic, public health, and public confidence implications, which
  require multi-jurisdictional preparation, prevention, response, and recovery efforts.

- Storage of processed and packaged goods represents another component of the farm-to-table continuum (see Figure 5). In this component, food products are stored in facilities before they are distributed to wholesalers, retailers, restaurants, and consumers. Depending on the scale of the storage and distribution facility, this component may represent a more regional vulnerability.

Figure 3 Local On-Farm Grain Storage

Figure 4 Feedlot

Figure 5 Chicken Ready for Consumer Purchase

Common Components

Common components exist within the wide variety of agricultural storage facilities. These components are consistent with the breakdown of facilities into storage of raw products, animal-slaughtering and -rearing facilities, and storage facilities for processed goods (see Table 1).

Table 1 Common Components in Various Types of Agricultural Facilities

Raw Product Storage Facility	Animal-Slaughtering and -Rearing Facility	Processed Storage and Distribution Facility
Storage bins	Open feed	Loading docks
Receiving lots	Slaughtering facilities	Large storage areas
Chemicals and fertilizers	Animal bins and pens	Transportation docks
Personnel	Transportation docks	Refrigeration components
—	Ventilation components	Specialized containers
—	Personnel	Personnel

Standards

Raw products, such as meat, poultry, fruits, vegetables, and dairy products, are stored in "cold storage" facilities, which are privately owned refrigerated warehouses. Currently, mandatory security guidelines have not been placed on these facilities, and inspection does not occur until the raw product reaches the food processor.

Raw grain is handled in one of two ways: roughly 50% is placed in on-farm storage, and the remaining 50% is placed in commercial grain bins. Depending on the market, grain may be moved from the field or farm storage to a county (local) elevator, terminal elevator, or processor. The grain is then checked for quality and segregated according to specific quality parameters. Currently, the U.S. Department of Agriculture (USDA) has not issued security guidelines for these facilities.

The Food Safety and Inspection Service (FSIS) of the USDA and the Food and Drug Administration (FDA) have prepared general food storage guidelines for industry. This guidance represents the thinking of these agencies on actions that could minimize the risk of tampering or intentional contamination. They are voluntary guidelines.

FSIS has provided two sets of guidelines:

- *FSIS Security Guidelines for Food Processors* (May 2002). Designed to assist federal- and state-inspected plants involved in meat, poultry, and egg production.

- *FSIS Safety and Security Guidelines for the Transportation and Distribution of Meat, Poultry, and Egg Products* (July 2003). Designed to assist small facilities in the shipping and handling of meat, poultry, and egg products.

These guidelines discuss issues such as planning; vulnerability assessment; development and implementation of procedures; emergency operations, training, and testing; employee screening and education; physical security; and operational security. These facilities, however, are not bound to incorporate these guidelines into existing security plans and may also use guidance from other government and private-sector organizations and agencies.

The FDA has provided the following guidance documents for industry:

- *Importers and Filers: Food Security Preventive Measures Guidance* (March 21, 2003);

- *Food Producers, Processors, and Transporters: Food Security Preventive Measures Guidance* (March 2003); and

- *Retail Food Stores and Food Service Establishments: Food Security Preventive Measures Guidance* (Draft: March 2003).

The FDA documents identify preventive measures that food handlers and establishments can use to minimize the risk of malicious, criminal, or terrorist actions. These documents are not mandatory; however, they offer guidelines for potential security violations that stem from activities related to management, human elements (employee and public), physical security, storage, and operations.

TERRORIST ACTIVITY INDICATORS

General Characteristics of Terrorist Surveillance

Terrorist surveillance may be fixed or mobile or both. 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; they may disguise themselves as street vendors, tourists, repair- or delivery persons, photographers, or even demonstrators to provide a plausible reason for being in the area.

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

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

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

Electronic surveillance, in this instance, refers to information gathering—legal and illegal—by terrorists using off-site computers. This type of data gathering might include information such as site maps, locations of key facilities, site security procedures, or passwords to company computer systems. In addition to obtaining information useful for a planned physical attack, terrorists may launch an electronic attack that could affect (e.g., damage or modify) data or software. Equipment and process controls could also be affected (e.g., damage a piece of equipment or cause an accident by opening or closing a track switch using off-site access to a 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 either be an end in itself or be launched simultaneously with a physical attack. Thus, it is worthwhile to be aware of what information is being collected from company and relevant government websites by off-site computer users and, if feasible, who is collecting this information. In addition, it is also important to know (if feasible) whether attempts are being made to gain access to protected company computer systems and whether any attempts have been successful.

Surveillance Indicators

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

Other Local and Regional Indicators

The remaining sets of indicators described in Exhibits 2–5 refer to activities not only in the immediate vicinity of the storage facilities, but also within a relatively large region around the agricultural storage facilities (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 storage facility of interest.

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	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 to find 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	Unusual aircraft flyovers of the facility.
	Continued on next page.

Activities Observed or Reported (Cont'd):	
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 activity 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 activity would be more important if the facility or asset is located in a rural area, rather than in or around a large city.
26	Traces of explosive or radioactive residue on facility vehicles during security checks 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.
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 targets (also applies to weapons of mass destruction [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 locations of the plant or place where the equipment is to be installed.
17	Reluctance to explain sufficiently what raw materials are to be used with the equipment.
18	Reluctance to provide clear answers to routine commercial or technical questions.
19	Reason for purchasing the equipment does not match the customer's usual business or technological level.
20	No request made or declines or refuses the assistance of a technical expert/training assistance when the assistance is generally standard for the installation or operation of the equipment.
21	Unable to complete an undertaking (due to inadequate equipment or technological know-how) and requests completion of a partly finished project.
22	Plant, equipment, or item is said to be for a use inconsistent with its design or normal intended use, and the customer continues these misstatements even after being corrected by the company/distributor.
23	Contract provided for the construction or revamping of a plant, but the complete scope of the work and/or final site of the plant under construction is not indicated.

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 of equipment used to modify weapons (silencers, etc.).
5	Theft, loss, or sales of large-caliber sniper weapons (.50 cal or larger).
6	Theft, sales, or reported seizure of night-vision equipment in combination with other indicators.
7	Theft, sales, or reported seizure of body armor in combination with other indicators.
8	Paramilitary groups carrying out training scenarios and groups advocating violence.
9	People wearing clothing that is not consistent with the local weather (also applicable under all other indicator categories).

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.
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.

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.

Chemical Agent Indicators:

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

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

USEFUL REFERENCE MATERIAL

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

2. *Terrorist Attack Indicators*, **HTML version**: [http://afsf.lackland.af.mil/Organization/ AFSFC/SFP/AF%20Pubs/Terrorist%20Attack%20Indicators]; **PDF version**: [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] (date accessed, Aug. 15, 2003).

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] (date accessed, Aug. 2003). 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] (date accessed, Aug. 2003). 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] (date accessed, Aug. 2003).

6. Princeton University, Department of Public Safety, *What is a Heightened Security State of Alert?* [http://web.princeton.edu/sites/publicsafety/] (date accessed, Aug. 15, 2003).

7. Kentucky State Police: Homeland Security/Counter-Terrorism, *Potential Indicators of WMD Threats or Incidents* [http://www.kentuckystatepolice.org/terror.htm] (date accessed, Aug. 18, 2003). 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] (date accessed, Aug. 15, 2003). 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* **2**(*3*) pp. 1–5, Feb. 12, 2003

[http://www.homelanddefensejournal.com/archives/pdfs/Feb_12_vol2_iss3.pdf] (date accessed, Aug. 2003).

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/].