POTENTIAL INDICATORS OF TERRORIST ACTIVITY INFRASTRUCTURE CATEGORY: NUCLEAR SPENT FUEL STORAGE 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 nuclear spent fuel storage facilities, which are located at operating and decommissioned nuclear power plant sites or at other locations throughout the United States).

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 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 and sometimes widely separated 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 the 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.

NUCLEAR SPENT FUEL STORAGE FACILITIES BACKGROUND

Terrorists Targeting Objectives

To consider terrorist threat indicators in relationship to used or "spent" nuclear fuel storage facilities, it is useful to understand the technologies and safeguards used to store spent nuclear fuel, where and how much spent fuel is currently stored, the nature of spent nuclear fuel, and why spent fuel facilities may be an attractive target for terrorist attack.

A terrorist attack on a nuclear spent fuel storage facility would be considered a significant security event. Although in a worst-case scenario, a successful terrorist strike could result in a release of highly radioactive material with the potential of contaminating persons and property in the downwind plume area, more realistic scenarios suggest that any contamination will be confined to the immediate area thus limiting the impact and significance of the release. Nevertheless, even if radioactive material were not released, widely held misconceptions of the potential consequences of a nonrelease attack on a nuclear spent fuel storage facility could have a significant negative impact.

In general, terrorists or terrorist groups may target a nuclear spent fuel storage facility to either (1) sabotage the facility or (2) divert radioactive or hazardous materials for other purposes[1], as depicted in Figure 1. As discussed above, facility sabotage could be to "weaponize" the facility against the surrounding population by attempting to cause a release of hazardous radioactive materials from the facility site. Facility sabotage might also be used to cause economic, national security, or logistical harm. Material diversion would most likely always be for weaponization to cause bodily harm or death, but not necessarily in the vicinity of the facility. Diverted radioactive materials or equipment might be used in their original form or for manufacturing other toxic, hazardous, explosive, or incendiary substances.

[1] Spent fuel in dry cask storage is less susceptible to diversion because of the massive weight and need for special rigging equipment to move the casks.

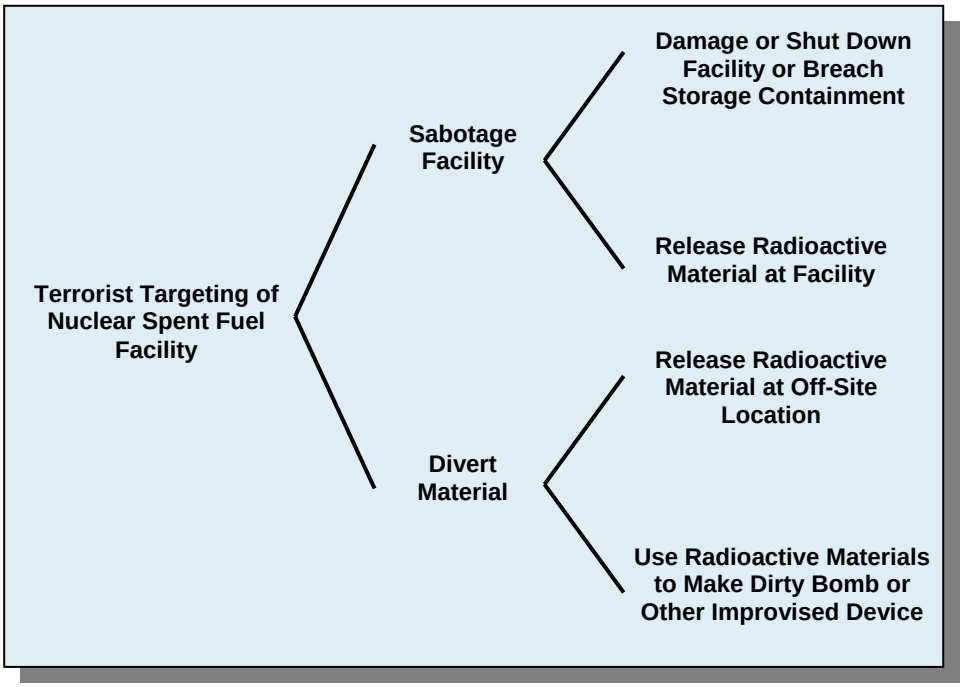
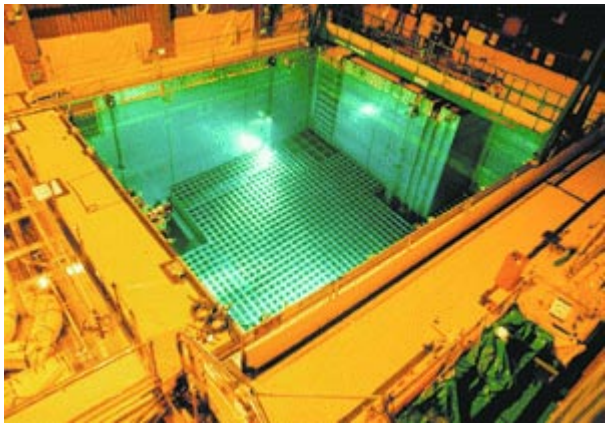


Figure 1 Terrorist Targeting Objectives for Nuclear Spent Fuel Storage Facilities

Sector Description

Nuclear fuel is composed of small, solid, ceramic pellets made of slightly enriched uranium held inside metal rods that are bundled together in what is called a fuel assembly. Fuel assemblies can be used for several years inside the reactor core before they must be replaced. Once they have been spent (or used), they must be shielded because they are highly radioactive. About one-fourth to one-third of the total fuel load from the pools is spent and removed from the reactor every 18 to 24 months and replaced with fresh fuel.

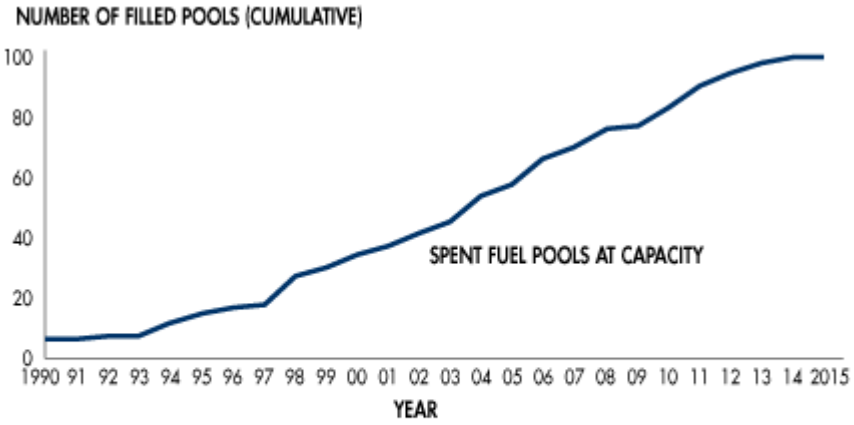
Spent radioactive nuclear fuel can be safely shielded with water or with steel and concrete. The U.S. Nuclear Regulatory Commission (NRC) allows two types of storage methods for spent nuclear fuel using these shielding methods (wet storage and dry cask). Wet storage involves placing the fuel assemblies in a large, deep pool filled with water inside a building on the plant site. Although similar in size to a large swimming pool, these pools are specially designed with at least 3-foot-thick concrete walls, steel liners, and mechanical equipment to cool the fuel, which gives off heat as well as radiation.



This water-pool option involves storing spent fuel rods under at least 25 feet of water, which

provides adequate shielding from the radiation for anyone near the pool. The rods are moved into the water pools from the reactor along the bottom of water canals, so that the spent fuel is always shielded to protect workers.

In the late 1970s and early 1980s, the need for alternative storage began to grow when pools at many nuclear reactors began to fill up with stored spent fuel. New NRC regulations, which permitted "re-racking" of the spent fuel pool grid and fuel rod consolidation, increased the amount of spent fuel that could be stored in the pool. However, both re-racking and consolidation are constrained by the size of existing spent storage pools. Figure 2 shows the current rate at which existing nuclear fuel storage pools will reach full capacity with re-racking and fuel rod consolidation.



Note: All operating nuclear power reactors are storing used fuel under NRC license in spent fuel pools. Some operating nuclear reactors are using dry cask storage. Information is based on loss of full-core reserve in the spent fuel pools.

Source: Energy Resources International and DOE/RW-0431 – Revision 1

Figure 2 Rate of Full Spent Fuel Storage Pools at U.S. Power Plants

Utilities began looking at options such as dry cask storage for increasing spent fuel storage capacity. Dry cask storage allows spent fuel that has already been cooled in the spent fuel pool for at least one year to be surrounded by inert gas inside a container called a cask. The casks are typically steel cylinders that are either welded or bolted closed. The steel cylinder provides leak-tight confinement of the spent fuel. Each cylinder is surrounded by additional steel, concrete, or another material to provide radiation shielding to workers and members of the public. Some of the cask designs can be used for both storage and transportation.

Dry storage is a passive system with no moving parts. The fuel is kept cool by air entering vents on the side of the concrete vault container and circulating around the outside of the steel

casks contained within. There are various dry storage cask system designs. With some designs, the steel cylinders containing the fuel are placed vertically in a concrete vault; other designs orient the cylinders horizontally. The concrete vaults provide the radiation shielding. Other cask designs orient the steel cylinder vertically on a concrete pad at a dry cask storage site and use both metal and/or concrete outer cylinders for radiation shielding. The first dry storage installation was licensed by the NRC in 1986 at the Surry Nuclear Power Plant in Virginia.

Spent fuel is currently stored in dry cask systems at a growing number of power plant sites and at an interim facility located at the Idaho National Environmental and Engineering Laboratory near Idaho Falls, Idaho. Figure 3 and Table 1 show the locations and types of licenses held by existing spent fuel storage facilities.

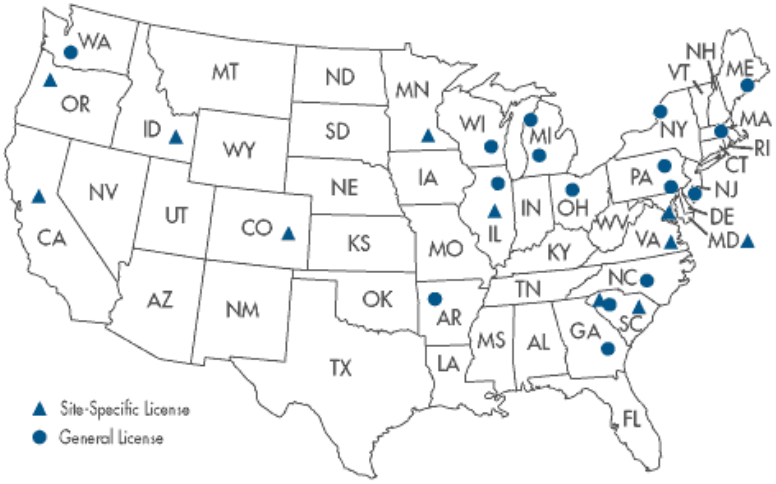


Figure 3 Locations of Nuclear Spent Fuel Facilities

Under a *site-specific license*, an applicant submits a license application to the NRC, and the NRC performs a technical review of all the safety aspects of the proposed facility. If the application is approved, the NRC issues a license that is valid for 20 years. A *general license* authorizes a nuclear power plant licensee to store spent fuel in NRC-approved casks at a site that is licensed to operate a power reactor under 10 CFR Part 50. Licensees are required to perform evaluations[2] of their site to demonstrate that the site is adequate for storing spent fuel in dry casks.

[2] These evaluations must show that the cask compliance and technical specifications can be met and include an analysis of earthquake intensity and tornado projectiles. The licensee must also review its security program, emergency plan, quality assurance program, training program, and radiation protection program and make any necessary changes to incorporate the storage facility at its reactor site.

Table 1 U.S. Nuclear Spent Fuel Facilities

State	Plant/Site Name	License Type
Arizona	Palo Verde	General
Arkansas	Arkansas Nuclear	General
California	Rancho Seco	Site-Specific
Colorado	Fort St. Vrain	Site-Specific
Georgia	Hatch	General
Idaho	DOE: TMI-2 Fuel Debris	Site-Specific
Illinois	GE Morris Dresden	Site-Specific General
Maine	Maine Yankee	General
Maryland	Calvert Cliffs	Site-Specific
Massachusetts	Yankee Rowe	General
Michigan	Palisades Big Rock Point	General General
Minnesota	Prairie Island	Site-Specific
New Jersey	Oyster Creek	General
New York	FitzPatrick	General
North Carolina	McGuire	General
Ohio	Davis-Besse	General
Oregon	Trojan	Site-Specific
Pennsylvania	Susquehanna Peach Bottom	General General
South Carolina	Oconee H.B. Robinson	General/Site-Specific Site-Specific
Virginia	Surry North Anna	Site-Specific Site-Specific
Washington	Columbia	General
Wisconsin	Point Beach	General

Source: U.S. Nuclear Regulatory Commission data as of March 2003

Radioactive Waste Materials

Terrorists may also be intent on diverting radioactive waste materials to assemble a dirty bomb or to otherwise release radioactive materials away from the nuclear plant site. In the U.S., radioactive waste is divided into three main types,[3,4] classified according to its activity, heat generation potential, and what it physically contains. These three main levels are low-level waste

[3] In most other countries, nuclear waste is categorized as LLW, intermediate-level waste, and HLW. The reason for this different classification system is that in the U.S., waste is classified on the basis of its origin. In most other countries, however, waste is classified according to the potential effects of the waste. In both classifications, LLW represents about 90% of all radioactive waste.

[4] A complete description of all three nuclear waste levels is included in the report entitled *Potential Indicators of Terrorist Activity Infrastructure Category: Nuclear Power Plants*.

(LLW), transuranic waste (TRU), and high-level waste (HLW). Although TRU would also be of interest to terrorists, spent fuel is included in the HLW category, which is described below.

The U.S. does not reprocess its spent fuel. Therefore, all the highly radioactive isotopes remain within the spent fuel, and the whole fuel assemblies are treated as HLW. The disadvantage of this "once-through" fuel cycle is that partially used nuclear fuel is treated as waste, thereby increasing the volume and complexity of disposal.

HLW is very radioactive, requires special shielding during handling and transport, and therefore could be targeted by terrorist groups. It also needs cooling, because it generates quite a lot of heat due to its high radioactivity level. A typical large nuclear reactor produces 25 to 30 tons of spent fuel per year. If the fuel were reprocessed and vitrified, the waste would be only about 3 cubic meters per year.

Transportation of Spent Fuel Assemblies

Very radioactive material like spent nuclear fuel is transported in "Type B" casks. Type B packages have at least 10 inches of shielding material to protect the environment from radiation and may weigh over 100 tons. They are certified by the NRC to withstand severe accident conditions as well as conditions of normal transportation.

These accident conditions include a drop of 30 feet onto an unyielding surface, a drop onto a metal pin 6 inches in diameter, an engulfing fire at 1,480°F that lasts 30 minutes, and immersion in water for eight hours. "Withstanding" these conditions means that in an accident producing these conditions, a container will not release more than the allowed amount of its radioactive contents.

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.

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

Surveillance Indicators

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

Other Local and Regional Indicators

The remaining sets of indicators described in Exhibits 2 to 5 refer to activities not only in the immediate vicinity of the facility but also to activities within a relatively large region around the facility (e.g., 100 to 200 miles). Local authorities should be aware of such activities and may not be able to associate them with a specific critical asset. 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	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 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.
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 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.

* The Fertilizer Institute developed a “Know Your Customer” program following the Oklahoma City incident. The information is available from TFI [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, 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, or an unexplained shortage in the area of baby formula (medium for growth).
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*, the html version of the file http://afsf.lackland.af.mil/Organization/AFSFC/SFP/AF%20Pubs/Terrorist%20Attack%20Indicators.PDF (Reference site removed prior to publication.).

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. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, *Locations of Independent Spent Fuel Storage Installations* [http://www.nrc.gov/waste/spent-fuel-storage/locations.html].

11. Connecticut Yankee Power Plant, *Used Fuel Storage* [http://www.connyankee.com/html/usedfuel_storage.html].

12. The New England Council, Inc., et al., *Responsible Nuclear Waste Disposal: An Unmet Obligation*, February 2001 [http://www.connyankee.com/Spent_Fuel_White_Paper_2002.PDF].

13. Sacramento Municipal Utility District, *Rancho Seco Fuel Move*, August 21, 2002 [http://www.smud.org/community/ranchoseco_fuelmove/].

14. Nuclear Energy Institute, *Nuclear Data – Used Fuel Storage*, available as links [http://www.nei.org/]. This site offers useful tutorials on nuclear energy and the nuclear fuel cycle in the United States; also contains summary statistics, ownership and financial data, and policy papers related to nuclear energy.

15. World Nuclear Association, *Information and Issue Briefs* [http://www.world-nuclear.org/info/info.htm#nuclearpower]. This site contains numerous articles about worldwide nuclear power and the nuclear fuel cycle.

16. American Nuclear Society, *Nuclear Science and Technology* [http://www.aboutnuclear.org/home.cgi]. This site offers a comprehensive summary of the nuclear industry in the United States, including pages on the history of the industry, radiation and radioactivity, nuclear wastes, and transportation.

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. U.S. Nuclear Regulatory Commission [http://www.nrc.gov/].
4. U.S. Department of Energy, Energy Information Administration [http://www.eia.doe.gov/].