POTENTIAL INDICATORS OF TERRORIST ACTIVITY INFRASTRUCTURE CATEGORY: HIGHWAY TUNNELS

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 highway tunnels, which provide critical transportation links through or under natural and man-made obstructions.

INTRODUCTION

Terrorist activity indicators are observable anomalies or incidents that may precede a terrorist attack or that may be associated with terrorist surveillance, training, planning, preparation, or mobilization activities. The observation of any one indicator may not, by itself, suggest terrorist activity. However, each observed anomaly or incident should be carefully considered along with all other relevant observations to determine whether further investigation is warranted. The objective is to look for items of information that fit together to form a relevant and credible picture of how a threat might become real at the infrastructure or asset 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 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 leading 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.

HIGHWAY TUNNELS BACKGROUND

Terrorists Targeting Objectives

To consider terrorist threat indicators in relationship to highway tunnels, it is useful to understand the demographics of highway tunnels in the United States, how tunnels are constructed, and why the tunnels might be attractive targets for terrorist attack. Highway tunnels provide critical transportation links under or through natural or man-made obstacles. Terrorists or terrorist groups may target tunnels to either (1) sabotage the tunnel and/or (2) delay or divert traffic for other purposes, as depicted in Figure 1. Sabotage could be for the purpose of causing bodily harm or death to vehicle occupants in the tunnel. Sabotage might also be for the purpose of causing long-term economic harm. The delay or diversion of traffic that normally uses a tunnel might also be an objective. Tunnels are usually critical transportation links, and diverting traffic from using a tunnel could impact the ability of emergency teams to respond to other (possibly, terrorist) incidents.

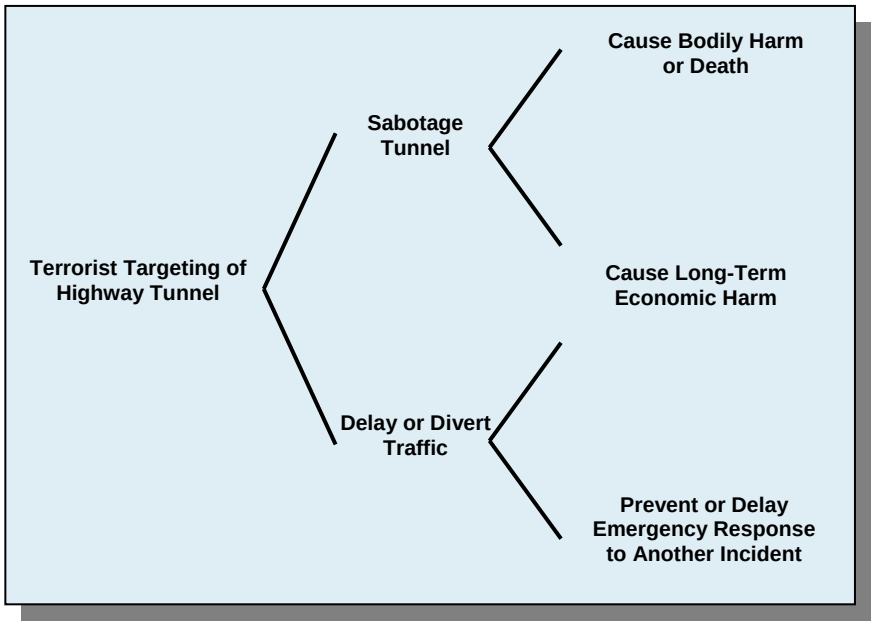

Figure 1 Terrorist Targeting Objectives for Highway Tunnels

Sector Description

Highway tunnels are enclosed passageways for road vehicles to travel through or under an obstruction, such as a city, mountain, river, or harbor. Tunnels may have one or more "tubes," and some are also equipped with rail lines for trains.

Highway tunnels are generally classified with regard to their method of construction: bored, cut and cover, or submerged. Tunnels through hard rock formations are usually bored (i.e., drilled) and finished to facilitate vehicular traffic. Very large boring machines are often used to cut the tunnel tubes through the hard rock formation.

Lincoln Tunnel, New York

Subway and shallow highway tunnels, especially in softer formations, may be constructed by using the cut and cover method. With this method, a large ditch is excavated, reinforced, finished, and then covered with overburden.

Tunnels that cross bodies of water may be bored through the bedrock beneath the water, or they may be constructed by submerging large prefabricated tube segments under the water and sealing them together before removing the water and finishing the roadbed. Whatever the construction method, tunnels are composed of a few major subsystems, including the tube, roadbed, lighting, intake and exhaust ventilation, monitors and sensors, and emergency exits.

Holland Tunnel, NY-NJ

There are 144 operating highway tunnels in the United States and 5 additional tunnel projects planned or under construction. Operating highway tunnels range in length from as long as 13,727 feet (2.6 miles) to as short as 75 feet. Of the 144 operating tunnels, 61 are longer than a quarter-mile in length, with approximately equal numbers in the 0.25-0.50 mile, 0.50-1.0 mile, and greater than 1.0 mile classifications. Also, 20 of the longest tunnels carry traffic under rivers, harbors, or other water bodies. Table 1 lists U.S. traffic tunnels that are longer than 0.25 mile.

Table 1 U.S. Highway Tunnels Greater Than One-Quarter Mile in Length

No.	Tunnel	Length	Year Opened	State	Immersed	Comment	Road
1	Anton Anderson Memorial	13,727	2000	AK		Road and railway tunnel. Whittier city.	
2	Brooklyn Battery	9,117	1950	NY	Yes	Second tube: 9,117 ft. East River. NYC.	
3	Eisenhower Memorial	8,960	1979	CO		First tube: 8,940 ft (1973). East portal 11,158 ft above sea level. World's highest road tunnel.	
4	Holland	8,556	1927	NY-NJ	Yes	Shortest tube: 8,369 ft Hudson river. NYC.	
5	Ted Williams	8,530	1995	MA	Yes	Two tubes. Immersed tunnel. Boston harbor.	I90
6	Lincoln Center	8,215	1937	NY	Yes	Hudson River. NYC.	
7	Lincoln South	8,005	1957	NY	Yes	Hudson River. NYC.	
8	Baltimore Harbor	7,651	1957	MD	Yes	Immersed tunnel.	I895
9	Hampton roads	7,480	1976	VA	Yes	Immersed tunnel (-100 ft). Second tube: 7,480 ft.	I764
10	Lincoln North	7,480	1945	NY	Yes	Hudson River. NYC.	
11	Fort McHenry	7,165	1985	MD	Yes	Immersed tunnel. Baltimore.	I95
12	Queens Midtown	6,414	1940	NY	Yes	Second tube: 6,273 ft. East River. NYC.	I495
13	Allegheny	6,070	1940/1965	PA		Second tube: 6,070 ft (1965). PA Turnpike.	I76
14	Thimble Shoal	5,735	1964	VA	Yes	Immersed tunnel. Chesapeake Bay.	US13
15	Liberty	5,689	1924	PA		Second tube: 5,689 ft. Pittsburgh.	
16	Sumner	5,659	1934	MA	Yes	Immersed tunnel. Boston. Opposite to Callahan.	1A
17	Chesapeake Channel	5,449	1999	VA	Yes	Shortest tube: 5,423 ft (1964). Immersed tunnel. Chesapeake Bay.	US13
18	East River Mountain	5,400	1974	VA - WV		Second tube: 5,400 ft.	I77
19	Tuscarora Mountain	5,325	1940	PA		Second tube: 5,325 ft (1968). PA Turnpike.	I76
20	Trans Koolau	5,279		HI		Second tube: 5,279 ft.	H3
21	Zion	5,249		UT			
22	Detroit - Windsor	5,131	1930	MI	Yes	Immersed tunnel (-75 ft). In USA: 1,647 ft.	Hwy 401
23	Callahan	5,069	1961	MA	Yes	Immersed tunnel. Boston. Opposite to Sumner.	1A
24	Wavona	4,839		CA		Yosemite.	RT41
25	Monitor Merrimac Memorial	4,800	1992	VA			I664
26	Kittatinny Mountain	4,728	1940	PA		Second tube: 4,728 ft (1968). PA Turnpike.	I76
27	Lehigh	4,462	1940	PA		Second tube: 4,380 ft (1991). PA Turnpike.	I76
28	Blue Mountain	4,341	1940	PA		Second tube: 4,341 ft (1968). PA Turnpike.	I76
29	Cumberland Gap	4,259	1986	TN-KY		Tunnel also underpasses part of Virginia.	

Continued on next page

No.	Tunnel	Length	Year Opened	State	Immersed	Comment	Road
30	Big Walker Mountain	4,229	1972	VA		Second tube: 4,229 ft.	I77
31	Squirrel Hill	4,226	1953	PA		Second tube: 4,226 ft. Pittsburgh.	I376
32	Midtown (2nd Norfolk Portsmouth)	4,193	1962	VA	Yes	Immersed tunnel (-90 ft).	
33	Devil's Slide	3,999	2006	CA		Two tubes. Work start: 2003.	US1
34	Downtown (1st Norfolk Portsmouth)	3,812	1987	VA	Yes	Shortest tube: 3,350 ft (1952). Immersed tunnel (-80 ft).	
35	Caldecott 1 & 2	3,615	1982	CA		Second tube: 3,610 ft.	US24
36	Fort Pitt	3,599	1960	PA		Second tube: 3,600 ft. Pittsburgh.	I 376
37	Posey Webster	3,547		CA		Second tube: 3,350 ft.	US24
38	I 95 - Mall	3,399	1073	DC		Second tube: 3,400 ft.	
39	Caldecott 3	3,369	1982	CA			US24
40	Wallace	3,110	1970	AL	Yes	Second tube: 3,110 ft. Under Mobile River.	I10
41	Bankhead	3,084	1950	AL	Yes	Two tubes. Under Mobile River.	US98
42	Berry Street	2,799	1997	PA		Pittsburgh.	
43	Wilson	2,625		HI		Oahu island.	SR63
44	Big Old Flat	2,477		CA		Yosemite.	RT41
45	Dewey Square	2,402		MA		Second tube: 2,400 ft. Boston.	
46	Route NJ 29	2,300	2002	NJ		Trenton.	NJ29
47	Broadway	1,969		CA		San Francisco.	
48	International Airport OC	1,909		CA			
49	Collier	1,886		CA			
50	Society Hill	1,804	1977	PA		Two tubes, 8 lanes.	
51	W105 – S405 Connector	1,781		CA			
52	Penn's Landing	1,700		DE		Second tube: 1,700 ft.	I95
53	9 th Street	1,611	1971	DC			
54	Bunyard (Bobby Hopper)	1,601	1999	AR			US71
55	Lowry Hill	1,496	1971	MN		Second tube: 1,496 ft. Minneapolis.	
56	Pine Mountain	1,434		NC		Second tube: 1,434 ft.	Blue Ridge Pkwy
57	Lindberg bvd.	1,417	2004	MO		St. Louis Airport.	
58	Fort Point Channel	1,401	2002	MA	Yes	Immersed tube. Boston.	I-90
59	Carlin Canyon	1,394	1975	NV		Two tubes, 4 lanes.	
60	E105 – N405 Connector	1,348		CA			
61	Mac Arthur	1,329		CA		San Francisco.	

TERRORIST ACTIVITY INDICATORS

General Characteristics of Terrorist Surveillance

Terrorist surveillance may be fixed or mobile. Fixed surveillance is done from a static, often concealed, position, possibly an adjacent building, business, or other facility. In fixed surveillance scenarios, terrorists may establish themselves in a public location over an extended period of time or choose disguises or occupations such as street vendors, tourists, repair or deliverymen, photographers, or even demonstrators to provide a plausible reason for being in the area.

Mobile surveillance usually entails observing and following persons or individual human targets, although it can be conducted against nonmobile facilities (i.e., driving by or through a tunnel to observe the facility or traffic). To enhance mobile surveillance, many terrorists have become more adept at progressive surveillance.

Progressive surveillance is a technique whereby the terrorist will observe a target for a short period of time from one position, withdraw for a time, possibly days or even weeks, and then resumes surveillance from another position. This activity continues until the terrorist develops target suitability and/or noticeable patterns in the operations or target's movements. This type of transient presence makes the surveillance much more difficult to detect or predict.

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

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

Electronic surveillance, in this instance, refers to information gathering, legal and illegal, by the terrorists using off-site computers. Such data gathering might include information such as site maps, locations of key facilities, site security procedures, or passwords to company computer systems. In addition to obtaining information useful for a planned physical attack, terrorists may launch an electronic attack that could affect data (e.g., damage or modify), software (e.g., damage or modify), or equipment/traffic controls (e.g., damage a piece of equipment).

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 overall 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 tunnels; most of the other indicator categories in this paper address activities in a much larger region around the tunnel 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 tunnel, but also activities within a relatively large region around the tunnel (e.g., 100 to 200 miles). Local authorities should be aware of such activities and may not be able to associate them with a specific critical asset because there may be several within the region being monitored. The objective is to look for items of information that fit together to form a relevant and credible picture of how a threat might become real at the tunnel 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	Non-facility persons showing an increased general interest in the area surrounding the facility.
8	Facility personnel willfully associating with suspicious individuals.
9	Computer hackers attempting to access sites looking for personal information, maps, or other targeting examples.
10	An employee who changes working behavior or works more irregular hours.
11	Persons observed or reported to be observing facility receipts or deliveries, especially of hazardous, toxic, or radioactive materials.
	(Continued on next page.)

Activities observed or reported:	
12	A noted pattern or series of false alarms requiring a response by law enforcement or emergency services.
13	Theft of facility or contractor identification cards or uniforms, or unauthorized persons in possession of facility ID cards or uniforms.
14	Recent damage (e.g., significant holes or cuts) to a perimeter fence or gate, or damage to perimeter lighting, security cameras, motion sensors, guard dogs, or other security devices.
15	Downloading of materials (e.g., maps, photographs, schematics, or similar materials) that could be used in conjunction with surveillance or attack planning activities.
16	Repeated attempts from the same location or country to access protected computer information systems.
17	Successful penetration and access of protected computer information systems, especially those containing information on site logistics, procedures, shipment schedules, security measures, passwords, and other sensitive information.
18	Attempts to obtain information about the facility (e.g., blueprints of buildings or information from public sources).
19	Unfamiliar cleaning crews or other contract workers with passable credentials; crews or contract workers attempting to access unauthorized areas.
20	A seemingly abandoned or illegally parked vehicle in the area of the facility or asset.
21	Increased interest in facility outside components (i.e., an electrical substation not located on site and not as heavily protected or not protected at all).
22	Sudden increases in power outages. This could be done from an off-site location to test the backup systems or recovery times of primary systems.
23	Increase in buildings being left unsecured or doors being left unlocked that are normally locked all the time.
24	Arrest by local police of unknown persons. This would be more important if facility or asset is located in a rural area rather than located in or around a large city.
25	Traces of explosive or radioactive residue on facility vehicles during security checks by detection swipes or devices.
26	Increase in violation of security guard standard operating procedures for staffing key posts.
27	Increase in threats from unidentified sources by telephone, postal mail, or through the e-mail system.
28	Increase in reports of threats from outside known, reliable sources.
29	Sudden losses or theft of guard force communications equipment.
30	Displaced or misaligned manhole covers or other service access doors on or surrounding the facility or asset site.
31	Unusual maintenance activities (e.g., road repairs) near the facility or asset.
32	Observations of unauthorized facility or non-facility personnel collecting or searching through facility trash.

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 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.

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 growth).
15	Break-ins/tampering at water treatment or food processing/warehouse facilities.
16	Solicitation for sales or theft of live agents/toxins/diseases from medical supply companies or testing/experiment facilities.
17	Persons stopped or arrested with unexplained lethal amounts of agents/toxins/ diseases/explosives.
18	Multiple cases of unexplained human or animal illnesses, especially those illnesses not native to the area.
19	Large number of unexplained human or animal deaths.
20	Sales (to nonagricultural users) or thefts of agricultural sprayers or crop dusting aircraft, foggers, river craft (if applicable), or other dispensing systems.
21	Inappropriate inquiries regarding local or regional chemical/biological sales/storage/transportation points.
22	Inappropriate inquiries regarding heating and ventilation systems for buildings/facilities by persons not associated with service agencies.
23	Unusual packages or containers, especially near heating, ventilating, and air-conditioning (HVAC) equipment or air intake systems.
24	Unusual powders, droplets, or mist clouds near HVAC equipment or air intake systems.
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, available at http://www.whitehouse.gov/pcipb/physical.html

2. *Terrorist Attack Indicators*, the html version of the file http://afsf.lackland.af.mil/Organization/AFSFC/SFP/AF%20Pubs/Terrorist%20Attack%20Indicators.PDF available at http://216.239.53.100/search?q=cache:YMHxMOEIgOcJ:afsf.lackland.af.mil/Organization/AFSFC/SFP/AF%2520Pubs/Terrorist%2520Attack%2520Indicators.PDF+terrorist+attack+indicators&hl=en&ie=UTF-8

3. U.S. Department of Homeland Security, *Potential Indicators of Threats Involving Vehicle Borne Improvised Explosive Devices (VBIEDs)*, Homeland Security Bulletin, May 15, 2003, available at http://www.apta.com/services/security/potential_indicators.cfm This document includes a table of chemicals and other demolitions paraphernalia used in recent truck bomb attacks against U.S. facilities.

4. U.S. Federal Bureau of Investigation, *FBI Community Outreach Program for Manufacturers and Suppliers of Chemical and Biological Agents, Materials, and Equipment*, available at http://www.vohma.com/pdf/pdffiles/SafetySecurity/ChemInfofbi.pdf This document includes a list of chemical/biological materials likely to be used in furtherance of WMD terrorist activities.

5. Defense Intelligence College, Counterterrorism Analysis Course, Introduction to Terrorism Intelligence Analysis, *Part 2: Pre-Incident Indicators*, available at http://www.globalsecurity.org/intell/library/policy/dod/ct_analysis_course.htm

6. Princeton University, Department of Public Safety, *What is a Heightened Security State of Alert?*, available at http://web.princeton.edu/sites/publicsafety/

7. Kentucky State Police: Homeland Security/Counter-Terrorism, *Potential Indicators of WMD Threats or Incidents*, available at http://www.kentuckystatepolice.org/terror.htm This site lists several indicators, protective measures, and emergency procedures.

8. U.S. Air Force, Office of Special Investigations, *Eagle Eyes: Categories of Suspicious Activities*, available at http://www.dtic.mil/afosi/eagle/suspicious_behavior.html This site has brief descriptions of activities such as elicitation, tests of security, acquiring supplies, suspicious persons out of place, dry run, and deploying assets.

9. Baybutt, Paul, and Varick Ready, *Protecting Process Plants: Preventing Terrorism Attacks and Sabotage*, **Homeland Defense Journal**, Vol. 2, Issue 3, pp. 1-5, Feb. 12, 2003, available at http://www.homelanddefensejournal.com/archives/pdfs/Feb_12_vol2_iss3.pdf

10. *The Worlds Longest Tunnel Page*, available at http://home.no.net/lotsberg/ .

11. Federal Emergency Management Agency, *HAZUS 99 User's Manual, Appendix C, Description of Lifeline Components*, available at http://home.no.net/lotsberg/ .

12. Nagasaki University, *Geo-Environment Laboratory*, available at http://www.gel.civil.nagasaki-u.ac.jp/data/method.html , this site has descriptions of many types of tunneling equipment and techniques.

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. National Transportation Library, http://ntl.bts.gov/reference_shelf.cfm
4. Transportation Research Board, http://www.trb.org/