

POTENTIAL INDICATORS OF TERRORIST ACTIVITY INFRASTRUCTURE CATEGORY: SUBWAYS

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 subways, which serve large United States (U.S.) cities and are characterized by high concentrations of people in closed environments that are vulnerable to attack.

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 subway system 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 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.

SUBWAY SYSTEM BACKGROUND

Terrorists Targeting Objectives

To consider terrorist threat indicators in relationship to subways, it is useful to understand the characteristics of U.S. subway systems and why these facilities might be attractive targets for terrorist attack.

A subway system, as defined here, includes not only the portion of a rail rapid transit system that is underground, but also the other portions of the rail rapid transit system, even if they are not beneath the ground surface. Data for U.S. subways are typically collected under the heading of “heavy rail,” which is an electric railway with the capacity to transport a heavy volume of passenger traffic and characterized by exclusive rights-of-way, multi-car trains, high speed, rapid acceleration, sophisticated signaling, and high-platform loading. Heavy rail is also known as “subway,” “elevated (railway),” or “metropolitan railway (metro).” Subway systems are typically only one division of a transit agency. Bus, light rail, and commuter rail often operate as feeders to subway stations.

Subways provide efficient and critical transportation links under, over, or through natural or manmade obstacles. Subways are potentially attractive targets because they have easy access, relatively little security, high concentrations of people in enclosed environments, moving trains, and ventilation shafts, station entrances, and exits above ground leading to an entire city.

Terrorists or terrorist groups may target subways to (1) cause bodily harm or death, and/or (2) cause serious economic harm, as depicted in Figure 1. Bodily harm or death could be accomplished by (1) a direct attack on the train with explosive devices, chemical weapons, biological weapons, or radiological weapons, or (2) releasing hazardous materials at the subway and thereby potentially affecting subway customers and employees as well as people at the surface near ventilation shafts and station entrances and exits. Serious economic harm could be accomplished through direct damage and destruction of the subway and/or by diverting, delaying, and snarling metropolitan traffic for a lengthy time during repairs and reconstruction.

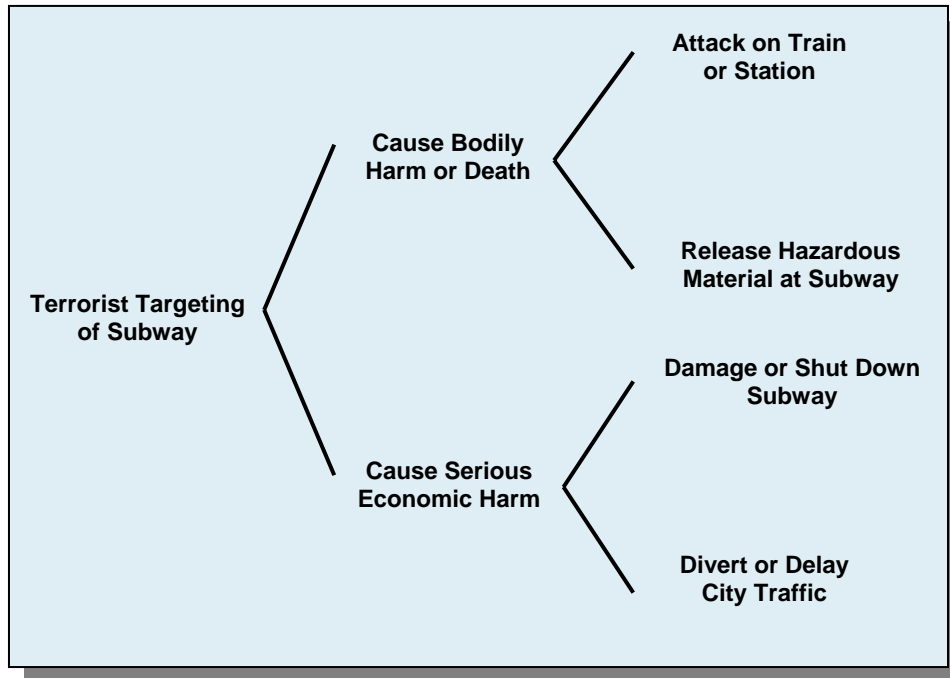


Figure 1 Terrorist Targeting Objectives for Subways

Sector Description

The U.S. has 14 major subway systems in 11 cities that are highly utilized for urban transport, as summarized in Table 1, where the systems are listed in order of passenger miles in 2001. There are over 1,500 right-of-way miles, over 1,000 stations, and over 10,500 vehicles in use. Approximately one-half of these subway stations are located underground. On an average day in the U.S., over 7 million passenger-trips are completed on these subway systems.

Table 1 shows that the largest systems in terms of daily one-way trips are New York, Washington, Chicago, Boston, and San Francisco, with the MTA – New York City Transit the largest by far, accounting for 64 percent of daily one-way trips and 58 percent of all passenger miles in the U.S.

All subway cars (except those in Cleveland and small sections of a branch in Chicago and Boston, which are powered by overhead cable) are powered by an electrified “third rail,” with a 600-volt capability. The inclusion of this third rail requires that subways be separated from other traffic for safety reasons by an exclusive right-of-way that does not interface with automotive or other passenger or freight cars.

Passenger service is not offered 24 hours per day on most subway systems. Transit agency activity is eventful during the early morning hours (track work, dispatchers, car maintenance, training, and cleaning). Large track renewal projects are generally undertaken in the spring and summer months.

DRAFT – SENSITIVE HOMELAND SECURITY INFORMATION
LAW ENFORCEMENT SENSITIVE

Table 1 Heavy Rail Transit Statistics for 2001

Primary City Served	Transit Agency	Right-of-way Miles	Average Daily One-Way Trips (millions)	Annual Passenger Miles (millions)	Total Vehicles	Fare Revenue (\$Million)	Operating Expenses (\$ Million)
New York, NY	MTA New York City Transit	494	4.77	8,274	6,195	1,524	2,212
Washington, DC	Washington Metropolitan Area Transit Authority	207	0.65	1,363	758	283	453
San Francisco, CA	San Francisco Bay Area Rapid Transit District	190	0.28	1,264	632	213	328
Chicago, IL	Chicago Transit Authority	206	0.50	1,009	1,190	153	339
Atlanta, GA	Metropolitan Atlanta Rapid Transit Authority	96	0.22	563	252	49	150
Boston, MA	Massachusetts Bay Transportation Authority	76	0.38	503	408	100	206
Philadelphia, PA	Southeastern Pennsylvania Transportation Authority	76	0.24	393	365	62	113
New York, NY	Port Authority Trans Hudson Corporation	25	0.22	338	335	89	149
Los Angeles, CA	Los Angeles County Metropolitan Transportation Authority	32	0.08	126	102	10	46
Miami, FL	Miami-Dade Transit Agency	42	0.04	108	136	11	58
Philadelphia, PA	Port Authority Transit Corporation	32	0.03	89	121	20	30
Baltimore, MD	Maryland Transit Administration	29	0.04	62	100	10	36
Cleveland, OH	Greater Cleveland Regional Transit Authority	38	0.02	62	60	6	27
New York, NY	MTA Staten Island Railway	29	0.01	25	64	4	26
TOTAL		1,572	7.47	14,178	10,718	2,533	4,171

Source: American Public Transportation Association. Obtained from <http://www.apta.com/research/stats/rail/index.cfm#A3>

Alternating current (AC) operates signals, station and tunnel lighting, ventilation, and miscellaneous line equipment. Direct current (DC) is used to operate trains and auxiliary equipment, such as emergency lighting. In New York City, the subway system has over 200 electrical-power substations that receive high- and low-voltage electrical current. Those substations may receive about 30,000 volts, and then convert it for use in the subway.

Tracks run above ground, below ground, and at elevations. Bridges, elevated structures, and tunnels carry the subway cars. Each subway system usually has one tunnel ventilation system that is equipped with thermostats, remote electric surveillance, and operations controls that allow the system to be used daily as well as in emergencies. During daily operations, a few fans are used, depending on traffic, temperature, and other parameters.

The length of a subway car ranges from 60-85 feet. Approximately 200 people can fit in a car. Typical subway trains are configured with two to six car sets, with cabs that are powered by traction motors at each end.

Each subway system has administrative offices, an operations control center, stations, maintenance facilities, and storage yards. The general layout of a subway station is shown in Figure 2.

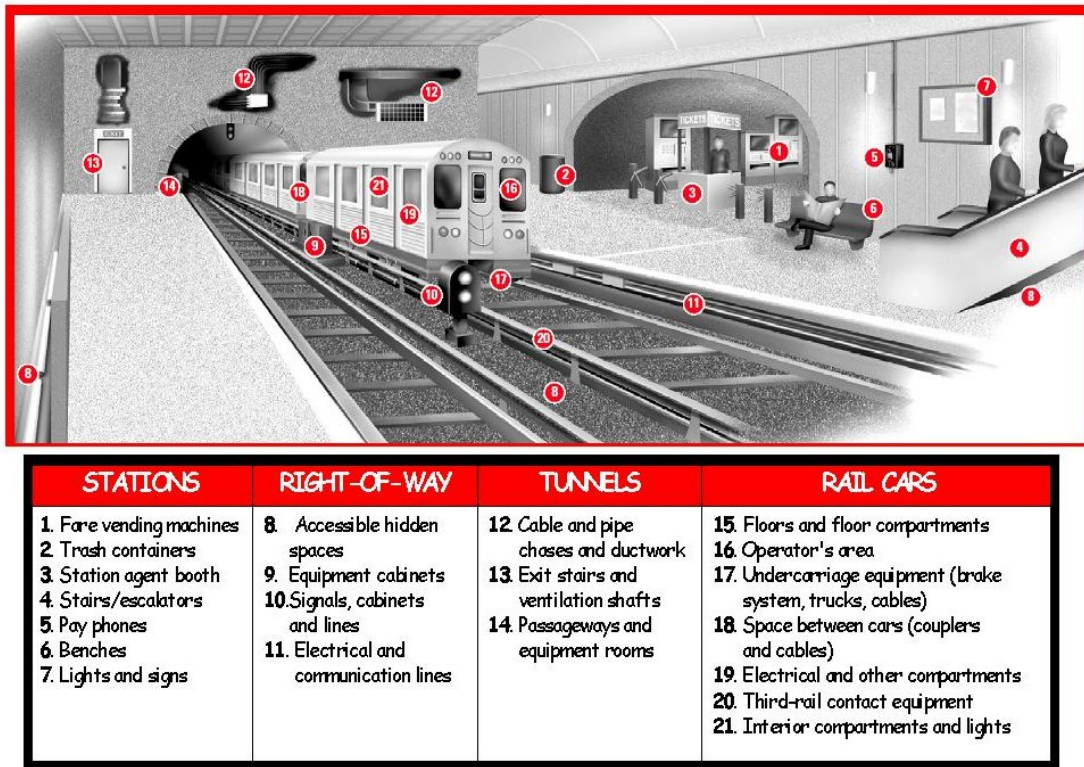


Figure 2 General Layout of a Subway Station
(Source: NTI Employee Guide to System Security for Heavy Rail Operations, Federal Transit Administration, National Transit Institute, Rutgers University)

TERRORIST ACTIVITY INDICATORS

General Characteristics of Terrorist Surveillance

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

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

Progressive surveillance is a technique whereby the terrorist observes a target for a short 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 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 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 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 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 subway; most of the other indicator categories in this report address activities in a much larger region around the subway system 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 subway, but also activities within a relatively large region around the subway (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 subway 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	
<i>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.</i>	
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.)	

DRAFT – SENSITIVE HOMELAND SECURITY INFORMATION
LAW ENFORCEMENT SENSITIVE

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	
<p><i>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.</i></p>	
<p>Transactional Indicators:</p> <p>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.</p>	
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 weapons of mass destruction).
13	Customer does not request a performance guarantee, warranty, or service contract where such is typically provided in similar transactions.
(Continued on next page.)	

DRAFT – SENSITIVE HOMELAND SECURITY INFORMATION
LAW ENFORCEMENT SENSITIVE

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	
<i>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.</i>	
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).

DRAFT – SENSITIVE HOMELAND SECURITY INFORMATION
LAW ENFORCEMENT SENSITIVE

Exhibit 4 Explosive and Incendiary Indicators	
<i>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.</i>	
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	
<i>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.</i>	
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.)	

DRAFT – SENSITIVE HOMELAND SECURITY INFORMATION
LAW ENFORCEMENT SENSITIVE

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. U.S. Department of Transportation, *Transportation Expressions*, available at <http://www.bts.gov/programs/btsprod/expr/expsearch.html> Definition for subway.
11. U.S. Department of Transportation, Bureau of Transportation Statistics, *National Transportation Statistics 2002*, available at <http://www.bts.gov/publications/nts/2002/index.html> Contains data on U.S. transportation systems. Appendix D defines heavy rail.
12. Jenkins, Brian M., and Larry N. Gersten, *Protecting Public Surface Transportation Against Terrorism And Serious Crime: Continuing Research On Best Security Practices*, Mineta Transportation Institute, San Jose, CA (September 2001), available at http://transweb.sjsu.edu/publications/terrorism_final.pdf
13. Federal Highway Administration, Federal Transit Administration, *Highway and Rail Transit Tunnel Inspection Manual*, March 2003, available at [http://assetmanagement.transportation.org/tam/aashto.nsf/All+Documents/DFBC8ACFF9BF5B1485256D11006498F7/\\$FILE/inspect.pdf](http://assetmanagement.transportation.org/tam/aashto.nsf/All+Documents/DFBC8ACFF9BF5B1485256D11006498F7/$FILE/inspect.pdf)
14. Mead, K. M., Inspector General, U.S. Department of Transportation, letter report to Frank Wolf, Chairman Subcommittee on Transportation and Related Agencies, Committee on Appropriations, U.S. House of Representatives, December 18, 2000. The subject of the 16-page letter report is a review of the Pennsylvania Station Redevelopment Project and conditions in the tunnels below the station.
15. Federal Transit Administration, *Guidelines for Managing Security Incidents Involving Surface Transit Vehicles*, Law Enforcement Sensitive/Official Use Only (August 2002).
16. National Institute of Justice, Federal Transit Administration, and National Nuclear Security Administration, *Guidelines for Managing Suspected Chemical and Biological Agent Incidents in Rail Tunnel Systems*, Law Enforcement Sensitive/Official Use Only (March 2002).

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. Department of Transportation, <http://www.dot.gov/>
4. U.S. Department of Transportation, Bureau of Transportation Statistics, <http://www.bts.gov/>
5. U.S. Department of Transportation, Federal Transit Administration, <http://www.fta.dot.gov/>
6. American Public Transportation Association, <http://www.apta.com/>
7. Metropolitan Transit Authority, State of New York, <http://www.mta.nyc.ny.us/>
8. New York City Subway Resources, <http://www.nycsubway.org/>
9. Washington Area Metropolitan Transit Authority, <http://www.wmata.com/>
10. Chicago Transit Authority, <http://www.transitchicago.com/>
11. Massachusetts Bay Transportation Authority, <http://www.mbta.com/>
12. San Francisco Bay Area Rapid Transit District, <http://www.bart.gov/index.asp?f=true>