POTENTIAL INDICATORS OF TERRORIST ACTIVITY INFRASTRUCTURE CATEGORY: BANKING SYSTEM PHYSICAL REPOSITORIES

Protective Security Division
Department of Homeland Security

DRAFT – Version 1, December 15, 2003

Preventing terrorism and reducing the nation's vulnerability to terrorist acts requires identifying specific vulnerabilities at critical sites, understanding the types of terrorist activities—and the potential indicators of those activities—that likely would be successful in exploiting those vulnerabilities, and taking preemptive and protective actions to mitigate vulnerabilities so that terrorists are no longer able to exploit them. This report discusses potential indicators of terrorist activity with a focus on banking system physical repositories, which supply, distribute, store, and ensure the security of U.S. currency, coins, and other market and clearing transactions.

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 repository 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 terrorists' choice of weaponry and the deployment method may help to eliminate certain classes of assets from the potential target spectrum. Except for geographic factors, however, such information alone may contribute little to identifying the specific target or targets. The best indicator that a specific site or asset may be targeted is direct observation or evidence that the site or asset is or has been under surveillance. Careful attention to the surveillance indicators, especially by local law enforcement personnel and asset owners, is an important key for identifying potential terrorist threats to a specific site or asset. To increase the probability of detecting terrorist surveillance activities, employees, contractors, and local citizens need to be solicited to observe and report the unusual activities, incidents, and behaviors highlighted in this report.

BANKING SYSTEM PHYSICAL REPOSITORIES BACKGROUND

Terrorist Targeting Objectives

To consider terrorist threat indicators in relationship to banking system physical repositories, it is useful to understand the characteristics of such repositories and why these facilities might be attractive targets for terrorist attack.

Terrorists or terrorist groups may target repositories 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 a direct attack on the repository with explosive devices, chemical weapons, biological weapons, or radiological weapons or by a release of hazardous materials in the repository, potentially affecting customers and employees, as well as third parties located outside the building at entrances and on adjacent sidewalks and streets. Serious economic harm could be accomplished through direct damage and destruction of the repository; theft of gold/silver bullion, bills, coins, printing plates, and financial instruments (e.g., gold certificates); compromising of the repository's electronic network systems to delay or halt check processing, electronic payments, distribution of bills and coins to local banks, and other electronic financial transactions.

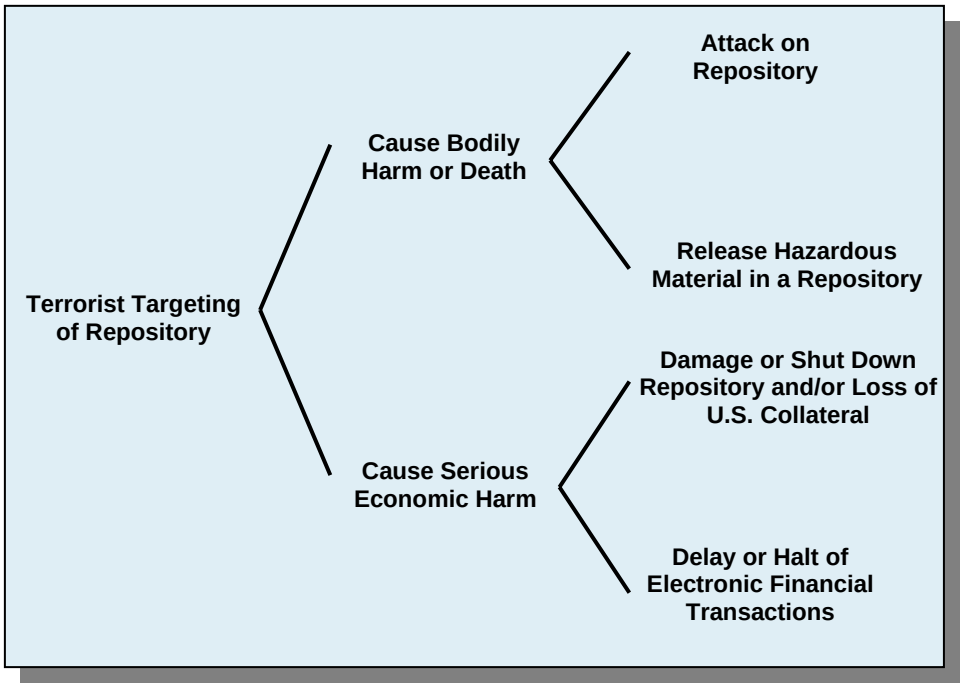


Figure 1 Terrorist Targeting Objectives for Banking System Physical Repositories

Sector Description

All currency notes and coins in the United States (U.S.) are produced by the Treasury Department. The Bureau of Engraving and Printing (BEP) produces currency notes, and the U.S. Mint produces coins (see photo). The Treasury Department must produce currency and coins in quantities that are sufficient to meet the needs of the public.

Bureau of Engraving and Printing, Washington, DC

The BEP has approximately 2,500 employees who work out of two buildings in Washington, DC, and a facility in Fort Worth, Texas. BEP functions include the following:

- Designing and manufacturing of U.S. currency;
- Designing and manufacturing of many postage stamps, customs stamps, and revenue stamps;

- Designing, engraving, and printing of Treasury bills, notes and bonds, and other U.S. securities; and
- Designing, engraving, and printing of commissions, permits, and certificates of awards.

The number of coins minted daily is astounding. Denver and Philadelphia alone produce 65 million to 80 million coins each day. The following sections briefly describe these and other facilities belonging to the U.S. Mint and the activities and responsibilities undertaken at each facility.

U.S. Mint Headquarters, Washington, DC

Functions performed at the U.S. Mint Headquarters include policy formulation and central agency administration, program management, research and development, marketing operations, customer services and order processing, operation of the Union Station sales center, business unit management, and all website services (www.usmint.gov).

Philadelphia Mint, PA

The nation's first mint provides a wide array of coin and manufacturing services. The Philadelphia Mint houses operations for engraving U.S. coins and medals; producing medal and coin dies, coins of all denominations for general circulation, the Philadelphia "P" mint mark portion of the annual uncirculated coin sets and commemorative coins authorized by Congress, and medals; giving public tours; and maintaining the facility's sales center. The Philadelphia Mint is currently the only facility that engraves the designs of U.S. coins and medals.

Denver Mint, CO

The Denver Mint produces coins of all denominations for general circulation, coin dies, and the Denver "D" mint mark portion of the annual uncirculated coin sets and commemorative coins authorized by the U.S. Congress; gives public tours (see photo); maintains the facility's sales center; and stores gold and silver bullion. Current output of the Denver Mint can exceed 50 million coins per day.

Tourists Gather for a Tour of the Denver Mint

San Francisco Mint, CA

The San Francisco Mint (see photo) plays an important role in our nation's coinage. Although it does not currently produce coins that are circulated, this mint is the exclusive manufacturer of regular proof and silver proof coin sets that establish the standard for numismatic excellence with their brilliant artistry, fine craftsmanship, and enduring quality.

U.S. Mint in San Francisco

West Point Mint, NY

The West Point Mint produces all uncirculated and proof one-ounce silver bullion coins; all sizes of the uncirculated and proof American Eagle gold bullion and platinum bullion coins; and all silver, gold, platinum, and bi-metallic commemorative coins authorized by Congress. The West Point Mint, located near the U.S. Military Academy in the State of New York, also stores silver, gold, and platinum bullion.

U.S. Fort Knox Bullion Repository, Fort Knox, KY

The Fort Knox Bullion Repository (see photo), located within the boundaries of the Fort Knox Military Reservation about 30 miles southwest of Louisville, stores U.S. gold bullion.

U.S. Bullion Repository, **Fort Knox, KY**

The two-story Depository building is constructed of granite, steel, and concrete. The bullion is contained in a two-level steel and concrete vault with numerous compartments. Opening the 20-ton vault door requires several staff members, each of whom is entrusted with part of the set of combinations for the locking system. The vault casing, including the roof, is constructed of steel plates, I-beams, and cylinders laced with hoop bands encased in concrete.

The vault is surrounded by a corridor, and offices and storerooms line the outer wall of the Depository building. The building's walls are constructed of granite lined with concrete. Four guard boxes are connected to the corners of the Depository building. There are sentry boxes at the entry gate in the steel fence, and a driveway circles the depository building. The building is equipped with its own backup power and water systems.

U.S. Mint Police

Responsibility for safeguarding U.S. gold and silver reserves lies with the U.S. Mint, which is part of the Treasury Department. The U.S. Mint Police are responsible for protecting government assets stored in the U.S. Mint facilities in Philadelphia, West Point, Denver, San Francisco, and Fort Knox. The U.S. Mint Police cooperate extensively with other law enforcement agencies. They use bicycle patrols around the mint facilities located in urban areas and have Special Response Teams that move among the facilities.

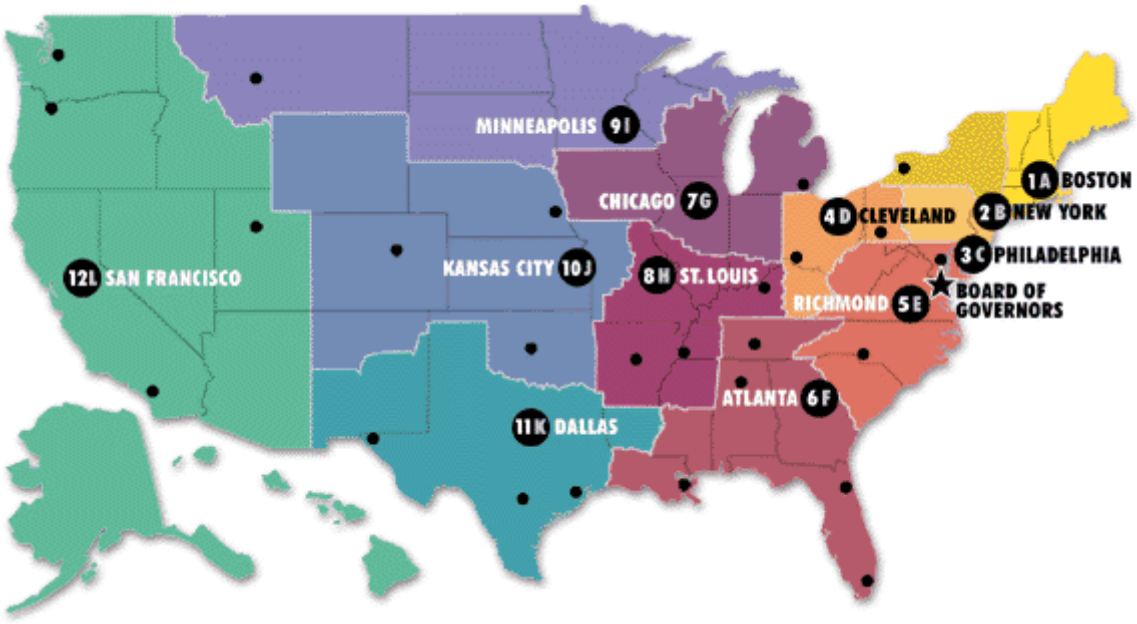
Federal Reserve Banks

Federal Reserve Banks are the operating arms of the Central Bank. They serve banks, the U.S. Treasury and, indirectly, the public. A Reserve bank is often called a "banker's bank," which means it stores currency and coins and processes checks and electronic payments. Reserve banks also supervise commercial banks in their regions. As the bank for the U.S. government, Reserve Banks handle the Treasury's payments, sell government securities, and assist with the Treasury's cash management and investment activities. A network of 12 Federal Reserve Banks and 25 branches make up the Federal Reserve System under the general oversight of the Board of Governors in Washington, DC (see Figure 2).

Each year, the currency departments at each of the 12 Federal Reserve Banks make recommendations as to future currency needs. The banks then place orders with the Comptroller of the Currency. The Comptroller reviews the requests and forwards them to the BEP. The BEP then produces the appropriate denominations of currency notes bearing the seal of the Federal Reserve Bank that placed the order. These Federal Reserve notes are claims on the assets of the issuing Federal Reserve Bank and liabilities of the U.S. government.

According to the law, each Federal Reserve Bank is required to hold collateral that equals at least 100% of the value of the currency it issues. Most of that collateral is in U.S. government securities owned by the Federal Reserve System. Collateral also includes gold certificates, special drawing rights, or other "eligible" paper, including bills of exchange or promissory notes and some foreign government or agency securities obtained by the Federal Reserve.

After production, the Treasury ships the coins and currency notes directly to Federal Reserve Banks and branches. The Federal Reserve then releases them as required by the commercial banking system. The demand for money by the public varies from week to week and from day to day. Banks are usually first to feel the impact of the public's demand for cash. To meet the needs of the public, banks turn to the regional Federal Reserve Bank for coins and currency when their supplies are low.



1 BOSTON	2 NEW YORK Buffalo	3 PHILADELPHIA	4 CLEVELAND Cincinnati Pittsburgh	5 RICHMOND Baltimore Charlotte	6 ATLANTA Birmingham Jacksonville Miami Nashville New Orleans
7 CHICAGO Detroit	8 ST. LOUIS Little Rock Louisville Memphis	9 MINNEAPOLIS Helena	10 KANSAS CITY Denver Oklahoma City Omaha	11 DALLAS El Paso Houston San Antonio	12 SAN FRANCISCO Los Angeles Portland Salt Lake City Seattle

Figure 2 Twelve Federal Reserve Banks and Their Branches

TERRORIST ACTIVITY INDICATORS

General Characteristics of Terrorist Surveillance

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

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

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

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

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

Electronic surveillance, in this instance, refers to information gathering—legal and illegal—by terrorists using off-site computers. This type of data gathering might include information such as site maps, locations of key facilities, site security procedures, or passwords to company computer systems. In addition to obtaining information useful for a planned physical attack, terrorists may launch an electronic attack that could affect (e.g., damage or modify) data or software. Equipment and process controls could also be affected (e.g., damage a piece of equipment or cause an accident by opening or closing a track switch using off-site access to a supervisory control and data acquisition [SCADA] system). Terrorists may also use technical means to intercept radio or telephone (including cell phone) traffic.

An electronic attack could 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 listed in Exhibit 1 are examples of unusual activities that should be noted and considered as part of an assimilation process that takes into account the quality and reliability of the source, the apparent validity of the information, and how the information meshes with other information on hand. For the most part, surveillance indicators refer to activities in the immediate vicinity of the repository; most of the other indicator categories in this report address activities in a much larger region around the repository 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 repository or even involving the repository directly, but also those within a relatively large region around the repository (e.g., 100 to 200 miles). Local authorities should be aware of such activities, although they may not be able to associate them with a specific critical asset because several may be within the region being monitored. The objective is to look for items of information that fit together to form a relevant and credible picture of how a threat might become real at the repository of interest.

EXHIBITS

Every attempt has been made to be as comprehensive as possible in listing the following terrorist activity indicators. Some of the indicators listed may not be specific to the critical infrastructure or critical asset category that is the topic of this report. However, these general indicators are included as an aid and reminder to anyone who might observe any of these activities that they are indicators of potential terrorist activity.

Exhibit 1 Surveillance Indicators Observed Inside or Outside an Installation	
What are surveillance indicators? Persons or unusual activities in the immediate vicinity of a critical infrastructure or key asset intending to gather information about the facility or its operations, shipments, or protective measures.	
Persons Observed or Reported:	
1	Persons using or carrying video/camera/observation equipment.
2	Persons with installation maps or facility photos or diagrams with facilities highlighted, notes regarding infrastructure, or a listing of installation personnel.
3	Persons possessing or observed using night vision devices near the facility perimeter or in the 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 target 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 flyovers in restricted airspace and boat encroachment into restricted areas, especially if near a repository.
	Continued on next page.

Activities Observed or Reported (Contd):	
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 (ID) 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's outside components (e.g., an electrical substation not located on-site and not as heavily protected or not protected at all).
23	Sudden increases in power outages. This activity could be done from an off-site location to test the backup systems or recovery times of primary systems.
24	Increase in unsecured buildings or unlocked doors that are normally locked at all times.
25	Arrest by local police of unknown persons. This activity would be more important if the facility or asset is located in a rural area, rather than in or around a large city.
26	Traces of explosive or radioactive residue on facility vehicles during security checks 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 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	An unusual customer request concerning the shipment or labeling of goods.
5	Packaging and/or packaging components that are inconsistent with the shipping mode or stated destination.
6	Unusually favorable payment terms, such as a higher price or better interest rate than the prevailing market or a higher lump-sum cash payment.
7	Unusual customer request for excessive confidentiality regarding the final destination or details of the product to be delivered.
8	Orders for excessive quantities of personal protective gear or safety/security devices, especially by persons not identified as affiliated with an industrial plant.
9	Requests for normally unnecessary devices (e.g., an excessive quantity of spare parts) or a lack of orders for parts typically associated with the product being ordered, coupled with an unconvincing explanation for the omission of such an order or request.
10	Sale canceled by customer but then customer attempts to purchase the exact same product with the same specifications and use, but using a different name.
11	Sale canceled by customer but then the identical product is stolen or “lost” shortly after the customer’s inquiry.
12	Theft/loss/recovery of large amounts of cash by groups advocating violence against government/civilian targets (also applies to weapons of mass destruction [WMD]).
13	Customer does not request a performance guarantee, warranty, or service contract where one 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 about the locations of the plant or place where the equipment is to be installed.
17	Reluctance to explain sufficiently what raw materials will 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 sale of large numbers of automatic or semi-automatic weapons.
2	Theft or sale 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 sale of large-caliber sniper weapons (.50 cal or larger).
6	Theft, sale, or reported seizure of night-vision equipment, in combination with other indicators.
7	Theft, sale, 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 sale 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	Sale or theft of large quantities, or an unexplained shortage in the area, of baby formula (medium for biological agent growth).
15	Break-ins/tampering at water treatment or food processing/warehouse facilities.
16	Solicitation for sale 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	Sale (to nonagricultural users) or theft of agricultural sprayers or crop dusting aircraft, foggers, river craft (if applicable), or other dispensing systems.
21	Inappropriate inquiries regarding local or regional chemical/biological sales/storage/transportation points.
22	Inappropriate inquiries regarding heating and ventilation systems for buildings/facilities by persons not associated with service agencies.
23	Unusual packages or containers, especially near HVAC equipment or air intake systems.
24	Unusual powders, droplets, or mist clouds near HVAC equipment or air intake systems.
Radioactive Material Indicators:	
25	Break-ins/tampering at facilities storing radioactive materials or radioactive wastes.
26	Solicitation for sale or theft of radioactive materials from medical or research supply companies or from testing/experiment facilities.
27	Persons stopped or arrested with unexplained radioactive materials.
28	Any one or more cases of unexplained human or animal radiation burns or radiation sickness.
29	Large number of unexplained human or animal deaths.
30	Inappropriate inquiries regarding local or regional radioactive material sales/storage/transportation points.

USEFUL REFERENCE MATERIAL

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

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

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 listing chemicals and demolitions paraphernalia used in recent truck bomb attacks against U.S. facilities.

4. U.S. Federal Bureau of Investigation, *FBI Community Outreach Program for Manufacturers and Suppliers of Chemical and Biological Agents, Materials, and Equipment* [http://www.vohma.com/pdf/pdffiles/SafetySecurity/ChemInfofbi.pdf] (date accessed, Aug. 20, 2003). This document includes a list of chemical/biological materials likely to be used in WMD terrorist activities.

5. Defense Intelligence College, Counterterrorism Analysis Course, *Introduction to Terrorism Intelligence Analysis, Part 2: Pre-Incident Indicators*, [http://www.globalsecurity.org/intell/library/policy/dod/ct_analysis_course.htm] (date accessed, Aug. 19, 2003).

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

7. Kentucky State Police: Homeland Security/Counterterrorism, *Potential Indicators of WMD Threats or Incidents* [http://www.kentuckystatepolice.org/terror.htm] (date accessed, Aug. 18, 2003). This site lists several indicators, protective measures, and emergency procedures.

8. U.S. Air Force, Office of Special Investigations, *Eagle Eyes: Categories of Suspicious Activities* [http://www.dtic.mil/afosi/eagle/suspicious_behavior.html] (date accessed, Aug. 18, 2003). This site has brief descriptions of activities such as elicitation, tests of security, acquiring supplies, suspicious persons out of place, dry run, and deploying assets.

9. Baybutt, Paul, and Varick Ready, "Protecting Process Plants: Preventing Terrorism Attacks and Sabotage," *Homeland Defense Journal* **2**(*3*):1–5, Feb. 12, 2003

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

10. U.S. Mint [http://www.usmint.gov] (date accessed, Aug. 18, 2003).

11. Bureau of Engraving and Printing [http://www.moneyfactory.com/] (date accessed, Aug. 15, 2003).

12. Federal Reserve Board [http://www.federalreserve.gov/] (date accessed, Aug. 18, 2003).

13. U.S. Treasury [http://www.ustreas.gov/] (date accessed, Aug. 15, 2003).

Related Websites

1. U.S. Department of Homeland Security [http://www.dhs.gov/dhspublic/index.jsp].
2. Federal Bureau of Investigation [http://www.fbi.gov/].