POTENTIAL INDICATORS OF TERRORIST ACTIVITY INFRASTRUCTURE CATEGORY: RAILROAD YARDS

Protective Security Division
Department of Homeland Security

Draft - Version 1, February 27, 2004

Preventing terrorism and reducing the nation's vulnerability to terrorist acts require 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 railroad yards.

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 railroad yard of interest and what it might look like. The key factor in 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.

RAILROAD YARD BACKGROUND

Terrorist Targeting Objectives

To consider terrorist threat indicators in relationship to railroad yards, it is useful to understand the basic structure of the industry and what general types of facilities might be attractive targets for terrorist attack. Railroad yards are attractive terrorist targets because they contain rail cars with toxic and hazardous materials that move extensively around the country. Figure 1 illustrates typical terrorist targeting objectives.

Casualties can be inflicted through the release of hazardous materials both in the yards and offsite. Damage or destruction of the facility can be intended to shut down or degrade the operation of the facility, or cause the release of hazardous materials to the surrounding area. Disruption of the facility without inflicting actual damage can be intended to interfere with facility operations and cause a decrease of output or to tamper with facility products to render them dangerous or unusable. Theft of equipment, materials, and products can be intended to divert them to other uses or to reap financial gain from their resale. Theft of information can be intended to acquire insight that is not made public or to gain data that can be used in carrying out attacks. Facility attacks can be intended to (1) cause economic, national security, or logistical harm; (2) contaminate product going into the food, medical, or health care system; or (3) "weaponize" the facility against the surrounding human population by causing the release of hazardous materials from the site.

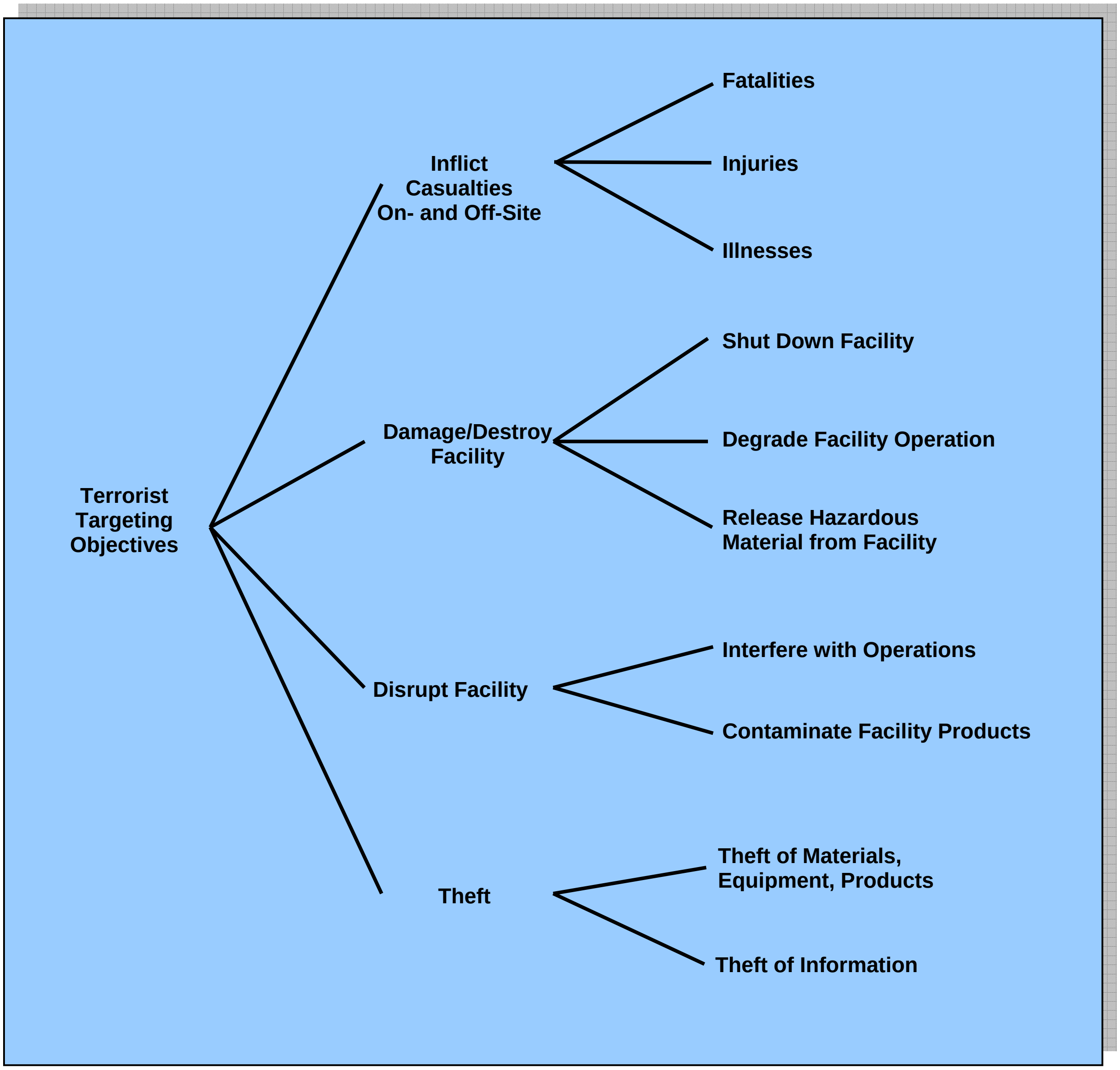

Terrorist Targeting Objectives
Inflict Casualties On- and Off-Site
Fatalities
Injuries
Illnesses
Damage/Destroy Facility
Shut Down Facility
Degrade Facility Operation
Release Hazardous Material from Facility
Disrupt Facility
Interfere with Operations
Contaminate Facility Products
Theft
Theft of Materials, Equipment, Products
Theft of Information

Figure 1 Potential Terrorist Targeting Objectives

Sector Description

Since virtually the first appearance of railroads in the United States (U.S.), rail carriers have used classification and sorting yards to enable efficient movement of freight for customers, shippers, and recipients. Railroad yards serve as hubs where loaded inbound rail cars on one line can be sorted and sent outbound on lines to their intended destinations. All types of traffic are handled in railroad yards. In recent years, however, traditional “loose car” processing has been increasingly superseded by unit trains of bulk commodities, such as coal or long-haul container trains that interchange motive power only between carriers and do not require yard service once dispatched from their origin. (Loose car processing refers to trains that consist of multiple “cuts” of both general- and special-purpose shipper-origin cars that are split in the yards and reorganized into recipient-destination trains.)

Currently, only seven major (i.e., revenue Class I) railroad carriers remain in the U.S. and Canada. The consolidation that resulted in this significant decrease in the number of large players in the industry has presented numerous opportunities for greater efficiency and service improvements, of which most carriers have taken full advantage. For example, because demand for re-sorting and classification operations is not growing significantly, rail carriers are increasingly finding it cost-effective to consolidate such operations at a limited number of facilities that may or may not be on their own property. Thus, two recent developments are of concern to vulnerability assessment:

- While more than 12 large new intermodal classification yards have gone into service in the U.S. and Canada in the last 10 years, the number of operating hump yards in North America has declined from 152 in 1975 to 58 today; several are used by carriers that neither own the property nor run the operation. Table 1 shows the distribution of classification yards by state.

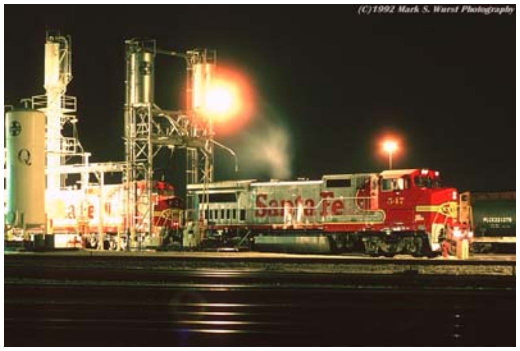
- The largest carriers are seeking to concentrate the yard operations they keep under their control, operations increasingly oriented to intermodal/container movements, at sites away from the traditional urban railroad hubs where land and operating costs can be high and security from theft and pilferage has been a chronic problem.

Table 1 Number of Active Hump Classification Yards by State

State	No.	State	No.	State	No.
Alabama	3	Maryland	1	Oklahoma	1
Arkansas	2	Minnesota	2	Oregon	1
California	4	Missouri	1	Pennsylvania	2
Georgia	3	Nebraska	1	Tennessee	3
Illinois	7	New Jersey	2	Texas	2
Indiana	3	New York	2	Virginia	2
Kansas	1	North Carolina	2	Washington	1
Kentucky	1	Ohio	5		

Source: http://www.trains.com.

Passive security in modern rail yards generally consists of high illumination by day and night, which enables good control of access to the property and minimizes the incidence of trespassing (Figures 2 and 3). Active security is accomplished by armed patrols and strategically placed video cameras. Perhaps counter-intuitively, it is likely that remote locations offer better potential security from human incursion because low surrounding population densities render the presence of unidentified persons or groups in the yard or its immediate vicinity more suspect.



(C)1992 Mark S. Wurst Photography

Figure 2 Rail Yard Illumination by Night

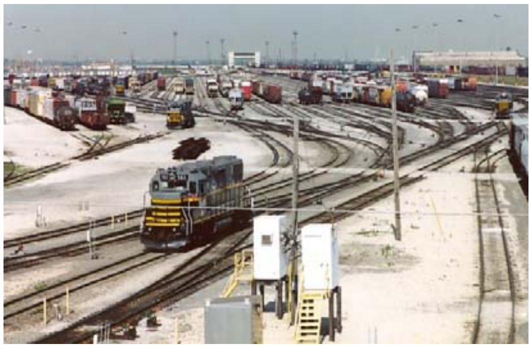


Figure 3 Rail Yard Illumination by Day

Common Facility Characteristics and Vulnerabilities

Railroad yards can be located in any type of environment having a flat area sufficiently extensive and elongated to permit emplacement of intermodal loading tracks, sorting "humps," classification "bowls," or any combination thereof. Thus, yard properties may be sited in open plains or adjacent to hills or other high ground (Figure 4). In the latter case, there may be vulnerabilities to adversaries using longer range, stand-off weapons.

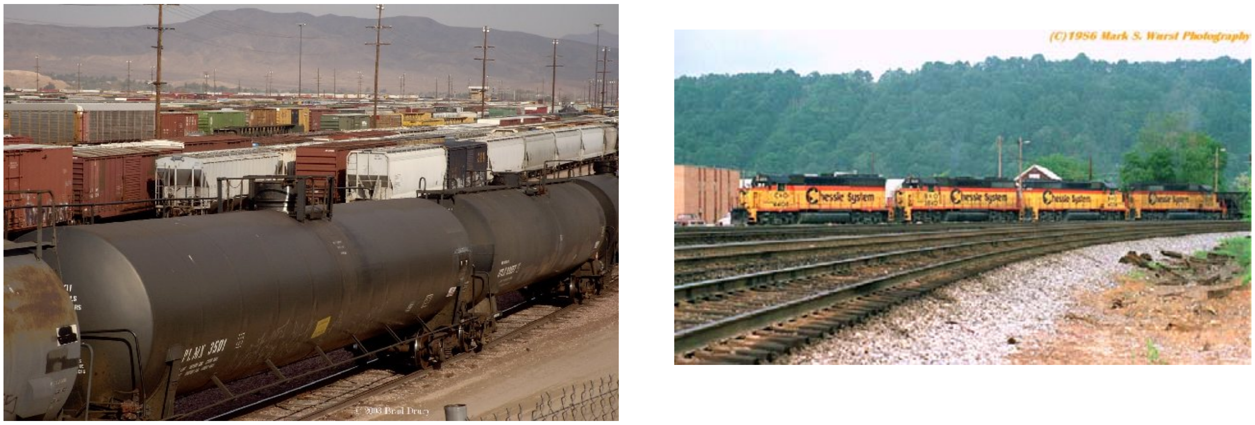


Figure 4 Rail Yard Sites Near Hills

Trains are put together in the classification yard, which is comprised of multiple parallel tracks branching out from a central track and connected by switches. Each of the parallel tracks is designated to receive cars with particular destinations along the route. A special locomotive, or switch engine, transports each car or group of cars to its assigned track. Depending on the sensitivity of the shipment and the type of classification yard, cars may be either "shoved to rest" or "humped." If shoved to rest, the car remains attached to the engine until it couples with the adjacent car. If humped, the car is uncoupled at the top of a very gentle incline and allowed to travel freely downhill.

Sorting humps are a central feature of large railroad yards that perform high-volume operations servicing many inbound and outbound trains daily. The hump exploits gravity to separate the components of an inbound train, one car at a time, into blocks that will be made into outbound trains with specific destinations. A locomotive pushes each car to the top of the hump (Figure 5). After the proper switches are thrown, the car is allowed to roll down to its assigned track in a multitrack classification area (often called a "bowl" because it has up-slopes at both ends to prevent runaways). In this area, thanks to wheel retarders on the hump down-slope, the car couples gently with the other cars in its outbound block. The optimal speed for coupling is 4 miles per hour, which can be achieved by either shoving or humping, although shoving to rest is more accurate. When all of the rail cars have been classified, the switch engine retrieves and connects them in the order given by the switch list.

Some very large yards have separate humps for eastbound (northbound) and westbound (southbound) operations. Yard operations, including hump classification, are controlled from a tower by the yardmaster, who has a 360-degree view of the operation (Figure 6).

© 2003 Brad Drury

Figure 5 Sorting Hump

©Rick Duncan, 2002

Figure 6 Control Tower

Most large yards also have a separate area for loading and unloading containers or truck trailers from flat cars. In recent years, new yards have opened in most major port cities and inland locations (e.g., Alliance Terminal near Ft. Worth, Texas; Willow Springs Yard, Illinois) expressly to handle intermodal traffic. Intermodal transshipment tasks are accomplished by overhead cranes or specially designed wheeled loaders (Figure 7). Generally, containers will be transshipped to or from highway trailers (flats) hauled to and from the yard by truck tractors. The latter units are operated by cartage company drivers or independent owner/operators (i.e., not railroad employees), who pick up or deliver the containers or trailers from or to points up to 100 miles or so distant that are not served by a rail spur.

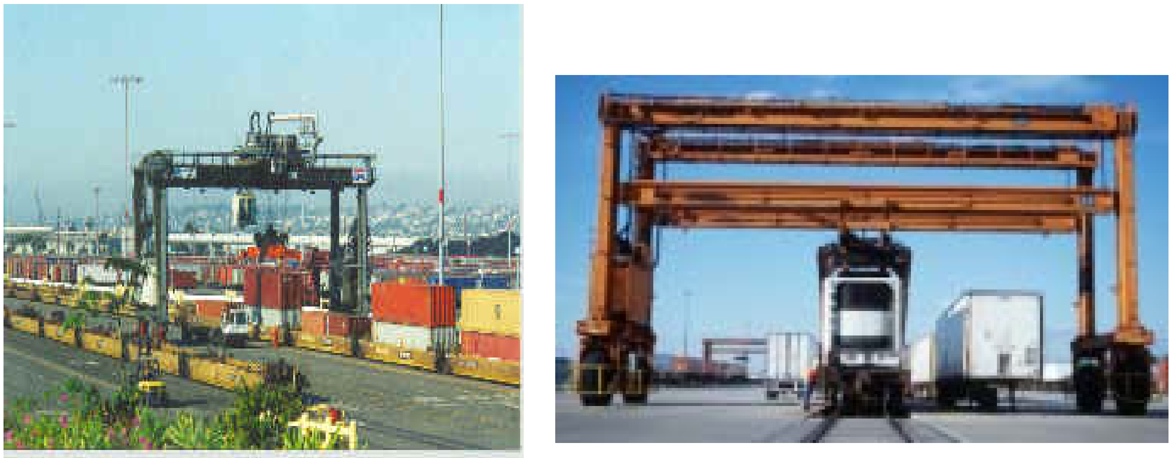


Figure 7 Intermodal Section of a Rail Yard with Crane and Loader

Many shipments processed through yards include military munitions and material. These shipments do not necessarily move in guarded trains (Figure 8). With respect to cyber security, cars being processed or laying over in yards are identified by their entry in computerized manifests and, occasionally, by on-board transponders. The actual contents of the cars could be concealed by cyber tampering, such as their deletion from car rosters.

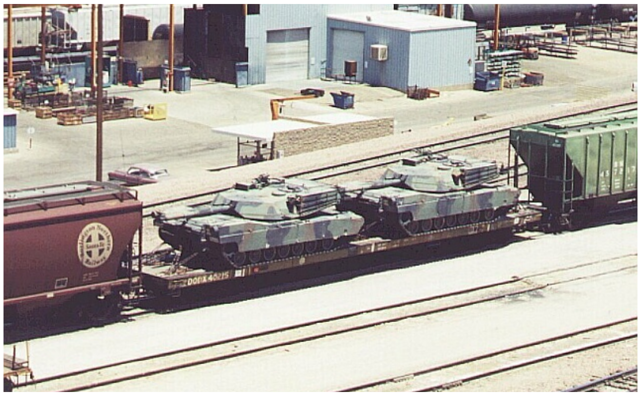


Figure 8 Military Shipment

Current yard surveillance systems are intended to prevent vandalism and theft of goods from rail cars during layovers, which can last 24 hours or more. Access to yards by authorized personnel or individuals who may accompany them or be admitted by their permission is not monitored at all times in all yards.[1]

Figure 9 shows a longitudinal view of a large railroad yard with a basic configuration that is still common today. It is possible to identify most of the features mentioned in this section.

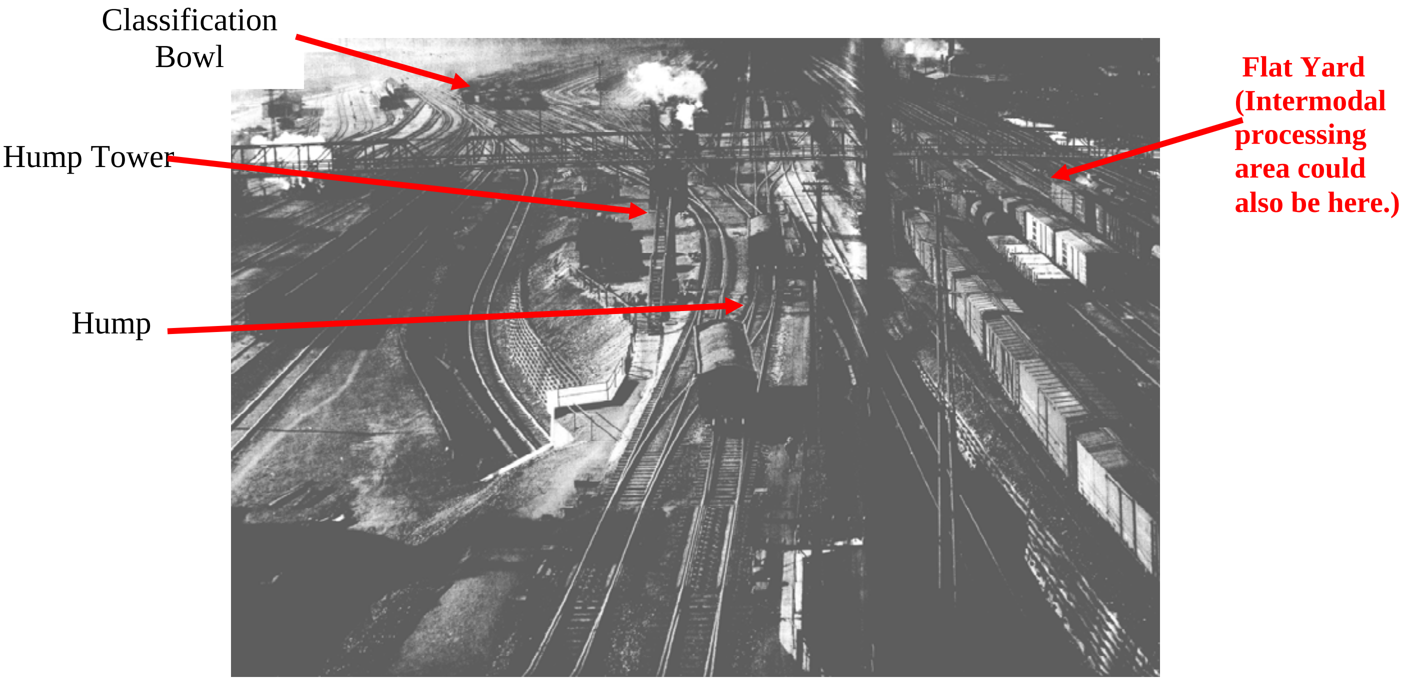


Figure 9 Longitudinal View of Railroad Yard with Basic Configuration

[1] Yard crews can occasionally include “utility employees” defined by 49 CFR 218.5 (Subpart A, Railroad Operating Practices) as “railroad employee(s) assigned to and functioning as a temporary member of a train or yard crew whose primary function is to assist the train or yard crew in the assembly, disassembly or *classification* of rail cars, or operation of trains.” FRA regulations (49 CFR 218.22) require only that such employees (a) be “subject to the Hours of Service Act, and (required) training and testing, control of alcohol and drug use, and hours of service record keeping, and (b) shall perform service as a member of only one train or yard crew at any given time. Service with more than one crew may be sequential, but not concurrent.”

TERRORIST ACTIVITY INDICATORS

There are several indicators of possible terrorist activity that should be monitored regularly. Constant attention to these indicators can help alert officials to the possibility of an incident.

Surveillance Indicators

Terrorist surveillance may be fixed or mobile. Fixed surveillance is conducted 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 individual human targets, although it can be conducted against nonmobile facilities (i.e., driving by a site to observe the facility or site operations). To enhance mobile surveillance, many terrorists have become more adept at progressive surveillance.

Progressive surveillance is a technique whereby the terrorist observes a target for a short time from one position, withdraws for a time (possibly days or even weeks), and then resumes surveillance from another position. This activity continues until the terrorist develops target suitability and/or noticeable patterns in the operations or 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 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. Public parks and other public gathering areas provide 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 and global positioning systems. It should be assumed that many terrorists have access to expensive 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 site maps, key facility locations, 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 damage or modify data, software, or equipment/process controls (e.g., cause a dangerous material release by opening or closing a valve using off-site access to the supervisory control and data acquisition [SCADA] system). Terrorists may also use electronic 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. It is also important to know whether attempts are being made to gain access to protected company computer systems and whether any attempts have been successful.

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

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 facility, but also those within a relatively large region around it (e.g., 100 to 200 miles). Local authorities should be aware of such activities but may not be able to associate them with a specific critical asset because several assets 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 facility of interest and what it might look like.

EXHIBITS

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

Exhibit 1 Surveillance Indicators Observed Inside or Outside an Installation

What are surveillance indicators? Persons or unusual activities in the immediate vicinity of a critical infrastructure or key asset intending to gather information about the facility or its operations, shipments, or protective measures.

Persons Observed or Reported:	
1	Persons using or carrying video/camera/observation equipment.
2	Persons with installation maps or facility photos or diagrams with facilities highlighted or notes regarding infrastructure or listing of installation personnel.
3	Persons possessing or observed using night vision devices near the facility perimeter or in the local area.
4	Persons parking, standing, or loitering in the same area over a multiple-day period with no apparent reasonable explanation.
5	Nonmilitary persons seen with military-style weapons and clothing/equipment.
6	Facility personnel being questioned off site about practices pertaining to the facility, or an increase in personal e-mail, telephone, faxes, or mail concerning the facility, or key asset.
7	Nonfacility persons showing an increased general interest in the area surrounding the facility.
8	Facility personnel willfully associating with suspicious individuals.
9	Computer hackers attempting to access sites looking for personal information, maps, or other targeting examples.
10	An employee who changes working behavior or works more irregular hours.
11	Persons observed or reported to be observing facility receipts or deliveries, especially of hazardous, toxic, or radioactive materials.
12	Aircraft flyover in restricted airspace; boat encroachment into restricted areas, especially if near critical infrastructure.

(*Continued on next page.)*

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

Exhibit 2 Transactional and Behavioral Indicators

What are transactional and behavioral indicators? Suspicious purchases of materials for improvised explosives or for the production of biological agents, toxins, chemical precursors, or chemicals that could be used in an act of terrorism or for purely criminal activity in the immediate vicinity or in the region surrounding a facility, critical infrastructure, or key asset.

Transactional Indicators

What are transactional indicators? Unusual, atypical, or incomplete methods, procedures, or events associated with inquiry about or attempted purchase of equipment or materials that could be used to manufacture or assemble explosive, biological, chemical, or radioactive agents or devices that could be used to deliver or disperse such agents. Also included are inquiries and orders to purchase such equipment or materials and the subsequent theft or loss of the items from the same or a different supplier.

1	Approach from a previously unknown customer or vendor (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 or vendor associated with or employed by a military-related business, such as a foreign defense ministry or foreign armed forces.
4	Unusual customer or vendor request concerning the shipment or labeling of goods. (e.g., offer to pick up shipment personally rather than arrange shipment and delivery).
5	Packaging and/or packaging components that are inconsistent with the shipping mode or stated destination.
6	Unusually favorable payment terms, such as a higher price or better interest rate than the prevailing market or a higher lump-sum cash payment.
7	Unusual customer or vendor 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 the customer or vendor but then the customer or vendor attempts to purchase the exact same product with the same specifications and use but using a different name.
11	Sale canceled by the customer or vendor 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).

(*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.*	
13	The customer or vendor does not request a performance guarantee, warranty, or service contract where such is typically provided in similar transactions.
14	Reluctance to give a sufficient explanation of the materials to be produced with the equipment and/or the purpose or use of those materials.
15	Evasive responses.
16	Reluctance to provide information on the plant locations 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 or training when the assistance is generally standard for the installation or operation of the equipment.
21	Unable to complete an undertaking (due to inadequate equipment or technological know-how) and requests completion of a partly finished project.
22	Plant, equipment, or item is said to be for a use inconsistent with its design or normal intended use, and the customer continues these misstatements even after being corrected by the company/distributor.
23	Contract provided for the construction or revamping of a plant, but the complete scope of the work and/or final site of the plant under construction is not indicated.
24	Theft of material or equipment with no practical use outside of a legitimate business facility or industrial process.
25	Apparent lack of familiarity with nomenclature, chemical processes, packaging configurations, or other indicators to suggest this person may not be routinely involved in purchasing chemicals.
26	Discontinuity of information provided, such as a phone number for a business, but the number is listed under a different name.
27	Unfamiliarity with the "business," such as predictable business cycles, etc.
28	Unreasonable market expectations, or fantastic explanations as to where the end product is going to be sold.

Exhibit 3 Weapons Indicators

What are weapons indicators? Purchase, theft, or testing of conventional weapons and equipment that terrorists could use to help carry out the intended action. Items of interest include not only guns, automatic weapons, rifles, etc., but also ammunition and equipment, such as night-vision goggles and body armor and relevant training exercises and classes.

Activities Observed or Reported:

1	Theft or sales of large numbers of automatic or semi-automatic weapons.
2	Theft or sales of ammunition capable of being used in military weapons.
3	Reports of automatic weapons firing or unusual weapons firing.
4	Seizures of modified weapons or 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.[1]
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 personnel using 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 a truck or van with minimum one-ton carrying capacity.
13	Modification of a 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.

[1] The Fertilizer Institute developed a "Know Your Customer" program following the terrorist incident at Oklahoma City. The information is available from TFI at http://www.tfi.org/.

Exhibit 5 Chemical, Biological, and Radiological Indicators

What are chemical, biological, and radiological indicators? Activities related to production, purchase, theft, testing, or storage of dangerous chemicals and chemical agents, biological species, and hazardous radioactive materials.

	Equipment Configuration Indicators:
1	Equipment to be installed in an area under strict security control, such as an area close to the facility or an area to which access is severely restricted.
2	Equipment to be installed in an area that is unusual and out of character with the proper use of the equipment.
3	Modification of a plant, equipment, or item in an existing or planned facility that changes production capability significantly and could make the facility more suitable for the manufacture of chemical weapons or chemical weapon precursors. (This also applies to biological agents and weapons.)
4	Suspicious packages, especially unexpected deliveries with no or an unknown return address and/or with excessive postage.
5	Unattended packages, briefcases, or other containers.
6	Unexpected or unfamiliar delivery trucks or deliveries.
7	Vehicles containing unusual or suspicious parcels or materials.
8	Theft, sale, or reported seizure of sophisticated personal protective equipment, such as “A”-level Tyvek, self-contained breathing apparatus (SCBA), etc.
9	Theft or sale of sophisticated filtering, air-scrubbing, or containment equipment
	Chemical Agent Indicators:
10	Inappropriate inquiries regarding local chemical sales/storage/transportation points.
11	Purchase or theft of explosives or restricted or sensitive chemicals.
12	Rental of self-storage units and/or delivery of chemicals to such units.
13	Chemical fires, noxious or toxic odors, brightly colored stains, or rusted metal fixtures in apartments, hotel rooms, or self-storage units.
14	Treated or untreated chemical burns or missing hands and/or fingers.
15	Unusual packages or containers, especially near heating, ventilating, and air-conditioning (HVAC) equipment or air intake systems.
16	Unusual powders, droplets, or mist clouds near HVAC equipment or air-intake systems.
	(*Continued on next page.)*

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

USEFUL REFERENCE MATERIAL

1. The White House, *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 file: [http://afsf.lackland.af.mil/Organization/AFSFC/SFP/AF%20Pubs/Terrorist%20Attack%20Indicators]; PDF file: [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 Information Bulletin*, May 15, 2003 [http://www.apta.com/services/security/potential_indicators.cfm]. This document includes a table of chemicals and other demolitions paraphernalia used in recent truck bomb attacks against U.S. facilities.

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

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

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

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

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

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

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. Agency for Toxic Substances and Disease Registry [http://www.atsdr.cdc.gov/].
4. Centers for Disease Control and Prevention [http://www.cdc.gov/].
5. U.S. Department of Commerce, Bureau of Industry and Security [http://www.bis.doc.gov/].
6. Trains Website [http://www.trains.com/Content/Dynamic/Articles/000/000/002/466szbkm.asp], accessed Feb. 2004.
7. Association of American Railroads Website, Freight Railroad Security Plan [http://www.aar.org/Rail_Safety/Rail_Security_plan.asp], accessed Feb. 2004.
8. TRANSCAER® Website, Strategic Plan [http://www.transcaer.org/public/about.cfm?about=plan], accessed Feb. 2004.