POTENTIAL INDICATORS OF TERRORIST ACTIVITY INFRASTRUCTURE CATEGORY: HOTELS

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 the hotel industry.

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 hotel 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.

HOTEL BACKGROUND

Terrorist Targeting Objectives

Specific threats of concern for hotels include:

- Explosives (e.g., car bomb, suicide bomber),
- Biological agents introduced into the facility (e.g., anthrax, botulism),
- Chemical agents introduced into the facility (e.g., chemical warfare agents, toxic industrial chemicals),
- Cyber attacks, and
- Arson.

Terrorists are most likely to choose vehicle bombs if their goal is to cause maximum casualties. This method has been used to attack hotels in the United States (U.S.) and around the world.

Hotels that are likely to be most vulnerable are those located in downtown areas of large cities, those hosting a controversial group or special event, those where U.S. or foreign dignitaries are guests, and those with a worldwide reputation and connections to a culture that is seen by some groups as corrupt (e.g., casino hotels).

An incident that illustrates hotel vulnerability occurred on January 16, 2004, when about 300 patrons were evacuated from a Melbourne, Australia, hotel after a noxious substance, possibly mace or pepper spray, was put in the heating, ventilating, and air-conditioning (HVAC) system. Only a few of the hotel patrons required hospital treatment. Four suspicious individuals were spotted on the hotel roof just prior to the incident.

Figure 1 depicts the range of possible objectives for a terrorist attack on hotel facilities. Damage or destruction of the hotel can be intended to inflict casualties, both on- and offsite, or to shut down or degrade the operation of the facility. Disruption of the facility without inflicting actual damage can be intended to interfere with operations. Theft of equipment, materials, or products can be intended to divert these items to other uses or 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.

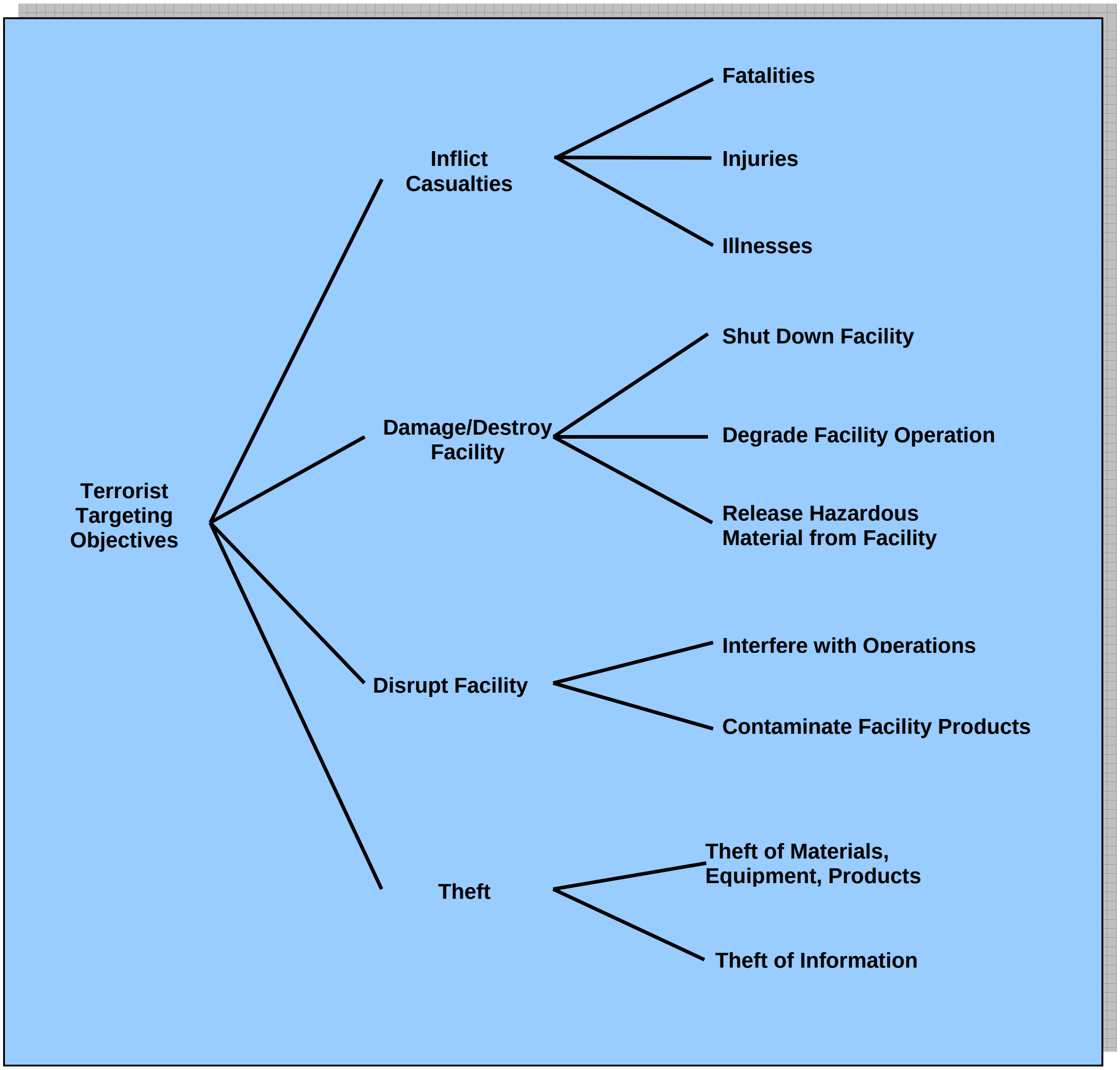
Terrorist Targeting Objectives
Inflict Casualties
Fatalities
Injuries
Illnesses
Damage/Destroy Facility
Shut Down Facility
Degrade Facility Operation
Release Hazardous Material from Facility
Disrupt Facility
Interfere with Operations
Contaminate Facility Products
Theft
Theft of Materials, Equipment,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

Figure 1 Potential Terrorist Targeting Objectives

Sector Description

In 2000, the American Hotel and Motel Association reported a total of 53,500 operating establishments with more than 4 million rooms. Industry-wide in 2003, the average occupancy rate was about 59%, with an average rate per room of about $84. Table 1 shows the breakdown of establishments, employees, and payroll among major types of lodging establishments. The hotel industry is a large sector in terms of employment and is the largest employer of people completing welfare-to-work programs, single parents, immigrants, and racial/ethnic minorities.

Table 1 U.S. Lodging Industry Statistics, 2000

Lodging Type	No. of Establishments	No. of Employees	Payroll ($M)
Hotels and motels	45,600	1,379,000	25,181
Casino hotels	300	312,000	8, 143
Bed and breakfast inns	3,000	19,000	254
Other facilities	900	5,000	83

Source: U.S. Census Bureau, *Statistical Abstract of the United States* (2002).

Demand for hotel rooms comes from both U.S. residents and foreign visitors; foreign visitors comprise a larger proportion of the total in cities such as New York and Washington, DC. The largest hotel market in the U.S. is Las Vegas, which has a total of about 128,000 rooms.

Table 2 shows the size distribution of lodging establishments in the U.S. Larger establishments, those with 75 or more rooms, make up about one-half of the total but account for nearly 80% of industry capacity.

Table 2 Lodging Establishments by Size and Total Capacity, 2000

No. of Rooms on Property	Establishments (%)	Rooms (M)
>500	1.3	11.2
300–500	2.8	9.9
150–299	10.9	21.3
75–149	33.5	35.1
<75	51.5	22.5

Source: U.S. Census Bureau, *Statistical Abstract of the United States* (2002).

Hotels can be characterized by price category and by location. Price categories generally employed are:

- Luxury, including super-luxury and luxury-deluxe;
- Upscale;
- Mid-rate;
- Economy; and
- Budget.

All-suite hotels may be found among the higher price categories, and extended-stay hotels are generally found among the lower price categories. Location categories include:

- Urban,

- Suburban,
- Airport,
- Highway, and
- Resort.

The cost of building a typical 500-room, mid-rate hotel is more than $50 million; construction and furnishings account for most of the cost. In 2002, new lodging industry construction in the U.S. surpassed $10 billion.

Table 3 lists the largest hotel companies, their hotel chains and worldwide establishments, and room capacity in 2002. Together, the largest companies account for about 29,000 establishments.

Table 3 Largest Hotel Companies Operating in the U.S. with Establishments and Rooms Worldwide, 2002

Company	Major Chains	No. of Establishments	No. of Rooms (1,000)
Cendant Corp.	Days Inn, Ramada (U.S.), Super 8, Howard Johnson, Travelodge	6,500	536
InterContinental Hotels Group	Holiday Inn, Inter-Continental	3,300	515
Marriott International	Marriott, Courtyard Residence Inn, Fairfield Inn, Renaissance, Ramada (non-U.S.)	2,600	471
Accor S.A.	Motel 6, Mercure, Ibis, Novotel, Red Roof Inns, Hotel Sofitel, Formule 1	3,800	441
Choice Hotels International	Comfort Inn, Quality Inn, Econo Lodge	4,700	376
Hilton Hotels	Hilton (U.S.), Hampton Inns, Doubletree, Embassy Suites, Homewood Suites	2,100	340
Best Western International	Best Western	4,100	308
Starwood Hotels & Resorts	Sheraton, Westin	700	228
Carlson Hospitality Group	Radisson, Country Inns & Suites by Carlson, Regent International Hotels	800	140
Hyatt Corp.	Hyatt Regency	100	60

Source: Standard and Poor's, *Industry Surveys: Lodging & Gaming*, August 7, 2003.

Hotel structures can be constructed in a variety of configurations, each of which has somewhat different vulnerabilities. Key configurations include atrium, tower, slab, and dispersed layouts.

Building configurations with guest rooms clustered around a central core or around a multistory atrium may be more vulnerable to several types of threats than those with individual units or low-rise clusters of rooms. Hotels may have vehicle parking beneath or within the structure. Hotels may also be integrated with other facilities, such as malls, casinos, convention centers, universities, and airports.

Figure 2 illustrates variations on a tower configuration with a central core. The distribution of functional areas within a tower configuration is illustrated in Figure 3.

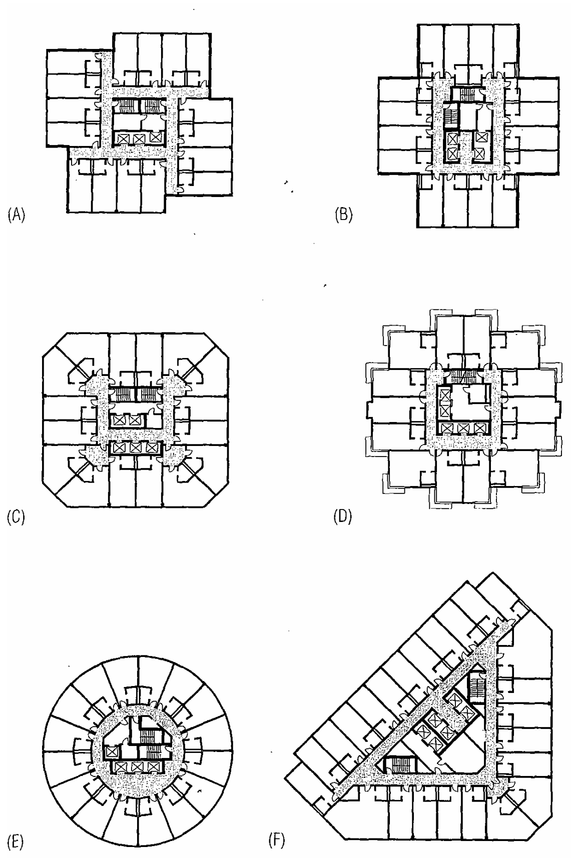

Figure 2 Tower Configurations with a Central Core (Source: Rutes et al., 2001)

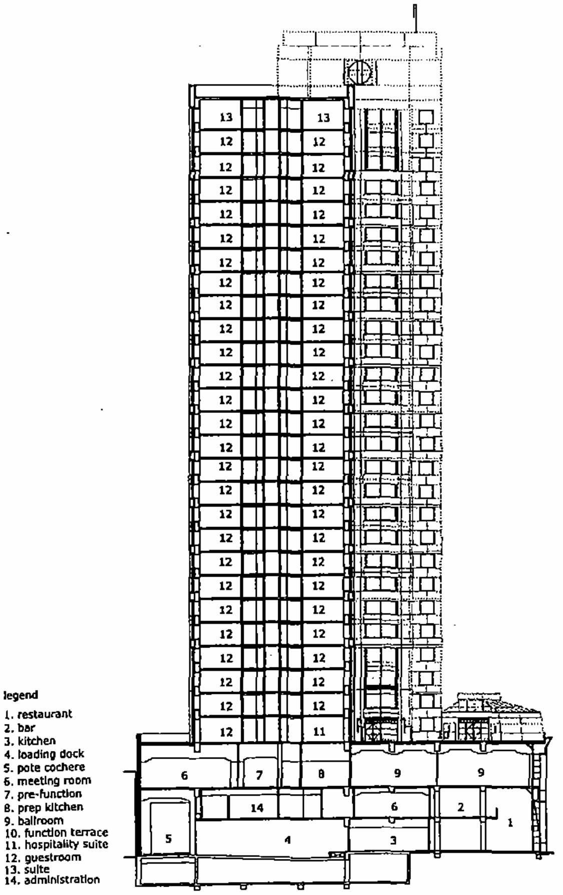

Figure 3 Arrangement of Functional Areas in a Tower Configuration (Source: Rutes et al., 2001)

Figure 4 shows two types of atrium layouts—open-ended and enclosed. Various slab configurations for hotel structures are shown in Figure 5.

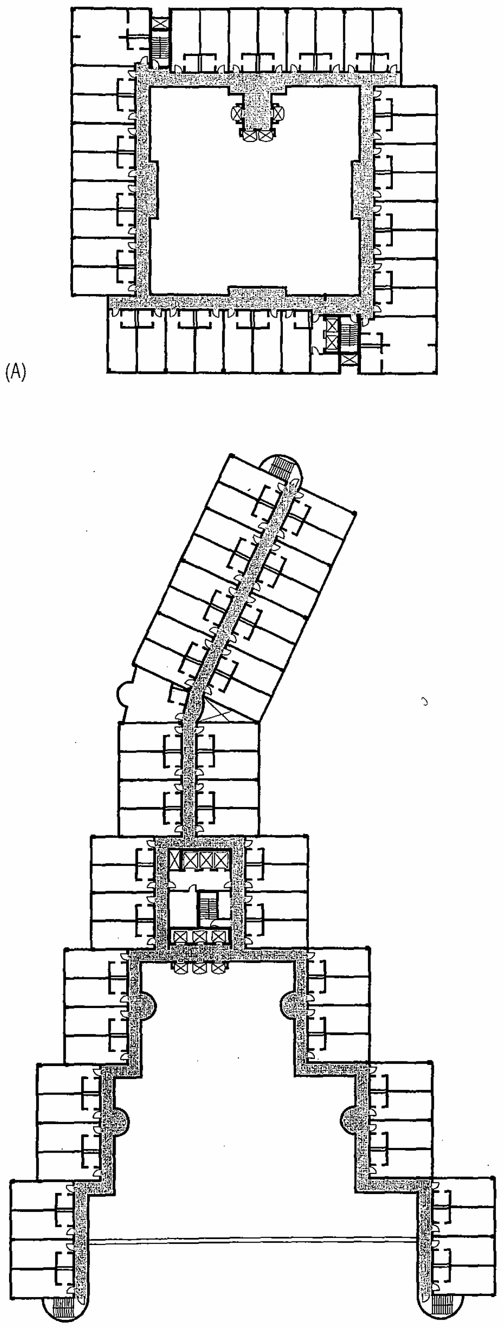

Figure 4 (a) Enclosed and (b) Open-ended Atrium Configurations (Source: Rutes et al., 2001)

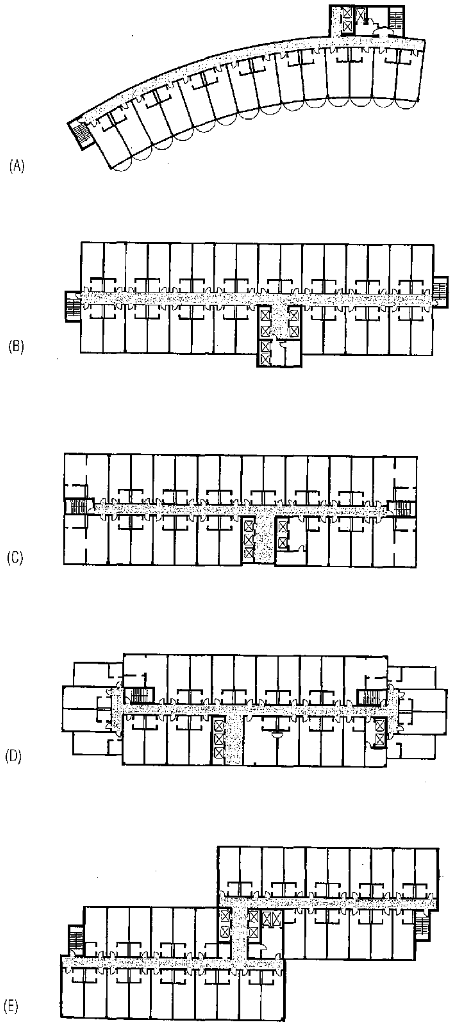

Figure 5 Slab Configurations for Hotel Structures (Source: Rutes et al., 2001)

Hotels generally have, and in some cases are required to have, both safety and security systems. Most hotels have systems in place to protect patrons' safety, including fire protection sprinklers and smoke detectors. Safety systems available for hotels include:

- Automatic fire detection and alarm systems;
- Automatic sprinklers;
- Central annunciator panels;
- Guest evacuation sound system;
- Fire-fighters' voice communication system;
- Smoke-proof, pressurized exit stairs; and
- Emergency generator for alarm systems, lighting, and smoke exhaust.

Security systems typically include electronic locks and in some cases surveillance cameras. A recent study by the Cornell School of Hotel Administration (Etz and Taylor, 2003) scored U.S. hotels on both a safety and a security index. The authors found that luxury and upscale hotels had the highest scores for both safety and security. In the economy and mid-price categories, newer hotels generally tended to have higher scores than older hotels. Hotel location and type also were related to safety and security scores. For instance, airport hotels tended to have high scores, whereas resort hotels tended to have very low scores. Conference and convention hotels and other large, full-service hotels tended to have relatively high scores, whereas smaller motels and bed and breakfast establishments had low scores.

The Department of Homeland Security (http://www.ussecassoc.com/public/docs/hsbulletin.htm) has issued a set of recommended security procedures for owners of soft targets, including public access buildings:

- Maintain situational awareness of world events and ongoing threats.
- Ensure all levels of personnel are notified via briefings, email, voice mail and signage of any changes in threat conditions and protective measures.
- Encourage personnel to be alert and immediately report any situation that may constitute a threat or suspicious activity.
- Encourage personnel to avoid routines, vary times and routes, pre-plan, and keep a low profile, especially during periods of high threat.
- Encourage personnel to take notice and report suspicious packages, devices, unattended briefcases, or other unusual materials immediately; inform them not to handle or attempt to move any such object.
- Encourage personnel to keep their family members and supervisors apprised of their whereabouts.
- Encourage personnel to know emergency exits and stairwells and rally points to ensure the safe egress of all employees.

- Increase the number of visible security personnel wherever possible.
- Rearrange exterior vehicle barriers, traffic cones, and road blocks to alter traffic patterns near facilities and cover by alert security forces.
- Institute/increase vehicle, foot, and roving security patrols varying in size, timing and routes.
- Implement random security guard shift changes.
- Arrange for law enforcement vehicles to be parked randomly near entrances and exits.
- Review current contingency plans and, if not already in place, develop and implement the following procedures: receiving of and acting on threat information; alert notification; terrorist incident response; evacuation; bomb threat; hostage and barricade; chemical, biological, radiological, and nuclear; consequence and crisis management; accountability, and media.
- When the aforementioned plans and procedures have been implemented, conduct internal training exercises and invite local emergency responders (fire, rescue, medical and bomb squads) to participate in joint exercises.
- Coordinate and establish partnerships with local authorities to develop intelligence and information sharing relationships.
- Place personnel on standby for contingency planning.
- Limit the number of access points, and strictly enforce access control procedures.
- Approach all illegally parked vehicles in and around facilities, question drivers and direct them to move immediately, if owner can not be identified, have the vehicle towed by law enforcement.
- Consider installing telephone caller I.D., record phone calls, if necessary.
- Increase perimeter lighting.
- Deploy visible security cameras and motion sensors.
- Remove vegetation in and around perimeters, maintain regularly.
- Institute a robust vehicle inspection program to include checking under the undercarriage of vehicles, under the hood, and in the trunk. Provide vehicle inspection training to security personnel.
- Deploy explosive detection devices and explosive detection canine teams.
- Conduct vulnerability studies focusing on physical security, structural engineering, infrastructure engineering, power, water, and air infiltration, if feasible.
- Initiate a system to enhance mail and package screening procedures (both announced and unannounced).
- Install special locking devices on manhole covers in and around facilities.

TERRORIST ACTIVITY INDICATORS

There are several indicators of possible terrorist activity that should be monitored on a regular basis. 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 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 obtaining 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 chemical 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 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 hotel; most of the other indicator categories address activities in a much larger region around the hotel.

Other Local and Regional Indicators

The sets of indicators described in Exhibits 2–5 refer to activities not only in the immediate vicinity of the facility, but also within a relatively large region around it (i.e., 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 of these 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 maps or facility photos or diagrams with assets highlighted or notes regarding infrastructure or listing of facility 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	Non-military 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 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 delivery schedules or locations.
12	People wearing clothing that is not consistent with the local weather.
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.
	(Continued on next page.)

15	Recent damage to door locks or doors, or damage to lighting, security cameras, 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 (e.g., HVAC system areas or roofs).
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 areas being left unsecured or doors being left unlocked that are normally locked all the time.
25	Unattended packages, briefcases, or other containers, especially near HVAC equipment or air intake systems.
26	Suspicious packages, especially unexpected deliveries with no or an unknown return address and/or with excessive postage.
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.
34	Unexpected or unfamiliar delivery trucks or deliveries.
35	Unusual powders, droplets, or mist clouds near HVAC equipment or air intake systems.

Exhibit 2 Transactional and Behavioral Indicators

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

Transactional Indicators:

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

1	Approach from a previously unknown customer (including those who require technical assistance) whose identity is not clear.
2	Transaction involving an intermediary agent and/or third party or consignee that is atypical in light of his/her usual business.
3	A customer associated with or employed by a military-related business, such as a foreign defense ministry or foreign armed forces.
4	Unusual customer request concerning the shipment or labeling of goods. (e.g., offer to pick up shipment personally rather than arrange shipment and delivery).
5	Packaging and/or packaging components that are inconsistent with the shipping mode or stated destination.
6	Unusually favorable payment terms, such as a higher price or better interest rate than the prevailing market or a higher lump-sum cash payment.
7	Unusual customer request for excessive confidentiality regarding the final destination or details of the product to be delivered.
8	Orders for excessive quantities of personal protective gear or safety/security devices, especially by persons not identified as affiliated with an industrial plant.
9	Requests for normally unnecessary devices (e.g., an excessive quantity of spare parts) or a lack of orders for parts typically associated with the product being ordered, coupled with an unconvincing explanation for the omission of such an order or request.
10	Sale canceled by customer but then customer attempts to purchase the exact same product with the same specifications and use but using a different name.
11	Sale canceled by customer but then the identical product is stolen or “lost” shortly after the customer’s inquiry.
12	Theft/loss/recovery of large amounts of cash by groups advocating violence against government/civilian sector targets (also applies to 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.)

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

Exhibit 3 Weapons Indicators

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

Activities Observed or Reported:

1	Theft or sales of large numbers of automatic or semi-automatic weapons.
2	Theft or sales of ammunition capable of being used in military weapons.
3	Reports of automatic weapons firing or unusual weapons firing.
4	Seizures of modified weapons or 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 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.

[1] The Fertilizer Institute developed a “Know Your Customer” program following the terrorist attack in 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 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 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 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].

10. American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc., *Report of Presidential Ad Hoc Committee for Building Health and Safety under Extraordinary Incidents on Risk Management Guidance for Health, Safety, and Environmental Security under Extraordinary Incidents*, Atlanta, GA, 2003 [http://buildingprotection.sbccom.army.mil/basic/index.htm].

11. American Society for Industrial Security International, "General Security Risk Assessment Guidelines," 2003 [http://www.asisonline.org].

12. Enz, C.A., and M.S. Taylor, *The Safety and Security of U.S. Hotels: A Post-September-11 Report*, The Center for Hospitality Research, Cornell School of Hotel Administration, 2003.

13. Federal Emergency Management Agency, *Reference Manual to Mitigate Potential Terrorist Attacks against Buildings*, FEMA 426 [www.fema.gov].

14. Lawrence Berkeley Laboratory, *Advice for Safeguarding Buildings against Chemical or Biological Attack*, 2003 [http://securebuildings.lbl.gov/].

15. National Institute for Occupational Safety and Health, *Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks*, DHHS (NIOSH) 2002-139, Department of Health and Human Services, Centers for Disease Control and Prevention, Cincinnati, OH, 2002 [http://www.cdc.gov/niosh/bldvent/2002-139.html].

16. Rusting Publications, *Protecting Hotels from Terrorism*, Westbury, NY, 2003.

17. Rutes, W.A., R.H. Penner, and L. Adams, *Hotel Design, Planning and Development*, W.W. Norton, New York, 2001.

18. *Tourism Tidbits* (newsletter) [http://www.unlv.edu/Tourism/tidbits.html].

19. U.S. Army Corps of Engineers, "Protecting Buildings and Their Occupants from Airborne Hazards," draft, TI853-01, Washington, DC, 2001 [http://buildingprotection.sbccom.army.mil/downloads/reports/airborne_hazards_report.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/].