U.S. Department of Homeland Security
Risk Management Division
Office of Infrastructure Protection

Hotels

In the United States, there are over 53,000 operating lodging establishments with more than 4 million rooms. Industry-wide in 2003, the average occupancy rate was about 59%. The industry employs more than 1.6 million people.

Potential Indicators of Terrorist Activity

Terrorists have a wide variety of weapons and tactics available to achieve their objectives. Specific threats of most concern to hotels include:

- Improvised explosive devices
- Arson
- Small arms attack
- Chemical/biological/radiological agent attack

Terrorist activity indicators are observable anomalies or incidents that may precede a terrorist attack. Indicators of an imminent attack requiring immediate action may include the following:

- Persons in crowded areas (e.g., hotel lobbies, common areas, restaurants) wearing unusually bulky clothing that might conceal suicide explosives
- Vehicles illegally parked near facility buildings or near places where large numbers of people gather
- Unattended packages (e.g., backpack, briefcase, box) that might contain explosives
- Suspicious packages and/or letters received by mail that might contain explosives or chemical/biological/ radiological agents
- Evidence of unauthorized access to HVAC areas of a building, such as indications of unusual substances (e.g., unknown powders, droplets, mists) near air intakes

Indicators of potential surveillance by terrorists include:

- Persons using or carrying video/camera/observation equipment in or near the hotel over an extended period
- Persons discovered with hotel maps, photos, or diagrams with critical assets highlighted or notes regarding infrastructure or listing of personnel
- Persons questioning hotel employees off-site about practices pertaining to the hotel and its operations, or an increase in personal e-mail, telephone, faxes, or postal mail requesting information about the facility or one of its key assets
- Hotel employees inquiring about facility operations, equipment, assets, or security measures about which they should have no job-related interest
- Hotel employees noted as willfully associating with suspicious individuals

Common Vulnerabilities

The following are key common vulnerabilities of hotels:

- *Unrestricted public access.* Openness to the general public is a feature common to hotels, and it contributes to the facility’s vulnerability.
- *Unrestricted access to peripheral areas.* Hotels can be vulnerable to attacks outside their buildings. Most have parking lots and/or parking garages where guests’ vehicles have access with little or no screening.
- *Unrestricted access to areas adjacent to buildings.* Most hotels have guest drop-off and pick-up points that are not distant enough to mitigate blasts from explosives in vehicles.
- *Limited employee background checks.* Many hotels, especially smaller ones, hire staff with little or no background checks.
- *Limited security force.* Many hotels have only a small security force.
- *Unprotected HVAC systems.* In some hotels, access to the HVAC systems is not controlled or monitored.
- *Building designs not security oriented.* Many hotel buildings are not designed with security considerations.
- *Multiple locations to place explosives or hazardous agents.* A hotel has numerous locations where an explosives package can be left without being immediately noticed.

Protective Measures

Protective measures include equipment, personnel, and procedures designed to protect a facility against threats and to mitigate the effects of an attack. Protective measures for hotels include:

- ### Planning and Preparedness
  - Designate an employee as security director to address all security-related activities.
  - Conduct threat analyses, vulnerability assessments, consequence analyses, risk assessments, and security audits on a regular and continuing basis. Develop a comprehensive security and emergency response plan.
  - Establish liaison and regular communication with local law enforcement and emergency responders.
  - Conduct regular exercises with hotel employees to test security and emergency response plans.

- ### Personnel
  - Conduct background checks on all employees.
  - Incorporate security awareness and appropriate response procedures for security situations into employee training programs.
  - Maintain an adequately sized, equipped, and trained security force.
  - Check guest identification upon check-in. Provide guests with information on how to report suspicious people or activities.

- ### Access Control
  - Define the hotel perimeter and areas within the hotel that require access control for pedestrians and vehicles.
  - Issue photo identification badges to all employees. Require that badge be displayed.
  - Issue special identification badges to contractors, cleaning crews, vendors, and temporary employees.
  - Restrict the storage of luggage to locations away from areas where large numbers of people congregate.

- ### Barriers
  - Install appropriate perimeter barriers and gates. Implement appropriate level of barrier security.
  - Install building perimeter barriers (e.g., fences, bollards, decorative flower pots, high curbs, shallow ditches).
  - Install barriers to protect doors and windows from small arms fire and explosive blast effects (e.g., blast-resistant and shatter-resistant glass, offset entryways).
  - Install vehicle barriers (e.g., bollards, fencing) to keep vehicles a safe distance from buildings and areas where large numbers of people congregate.

- ### Communication and Notification
  - Install systems that provide communication with all people at the hotel, including employees, security force, emergency response teams, and guests.
  - Install systems that provide communication channels with law enforcement and emergency responders.

- ### Monitoring, Surveillance, Inspection
  - Install video surveillance equipment (e.g., closed-circuit television [CCTV], lighting, night-vision equipment).
  - Continuously monitor all people, including guests, entering and leaving the facility.
  - Consider acquiring luggage-screening equipment for use during high-threat and/or high-profile events.
  - Implement quality control inspections on food supply to hotel restaurants and special events.

- ### Infrastructure Interdependencies
  - Ensure that the hotel has adequate utility service capacity to meet normal and emergency needs.
  - Ensure that employees are familiar with how to shut off utility services (e.g., electricity, natural gas) in emergency situations.

- ### Cyber Security
  - Develop and implement a security plan for computer and information systems hardware and software.
  - Regularly review the hotel's Web site to ensure no sensitive information is provided.

- ### Incident Response
  - Ensure that an adequate number of emergency response personnel are on duty and/or on call at all times.
  - Identify alternate rallying points where employees and others at the facility can gather for coordinated evacuation and/or for "head counts" to ensure all have been evacuated.

More detailed information on hotels is contained in the document, *Hotels: Potential Indicators of Terrorist Activity, Common Vulnerabilities, Protective Measures.* Information on issues relevant to a wide range of critical infrastructures and key resources is available in the document, *Overview of Potential Indicators of Terrorist Activity, Common Vulnerabilities, and Protective Measures for Critical Infrastructures and Key Resources.* Both are available from the contacts below.

WARNING

This document is **FOR OFFICIAL USE ONLY (FOUO).** It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

At a minimum when unattended, this document is to be stored in a locked container such as a file cabinet, desk drawer, overhead compartment, credenza or locked area offering sufficient protection against theft, compromise, inadvertent access and unauthorized disclosure.

For more information about this document contact:
Wade Townsend (703-235-5748
Wade.Townsend@dhs.gov)