CHARACTERISTICS AND COMMON VULNERABILITIES INFRASTRUCTURE CATEGORY: HOTELS

Protective Security Division
Department of Homeland Security

Draft - Version 1, February 13, 2004

Preventing terrorism and reducing the nation's vulnerability to terrorist acts require understanding the common vulnerabilities of critical infrastructures, identifying site-specific vulnerabilities, understanding the types of terrorist 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 characterizes and discusses the common vulnerabilities of hotel facilities.

POTENTIAL THREATS

Specific threats that are of concern to 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.

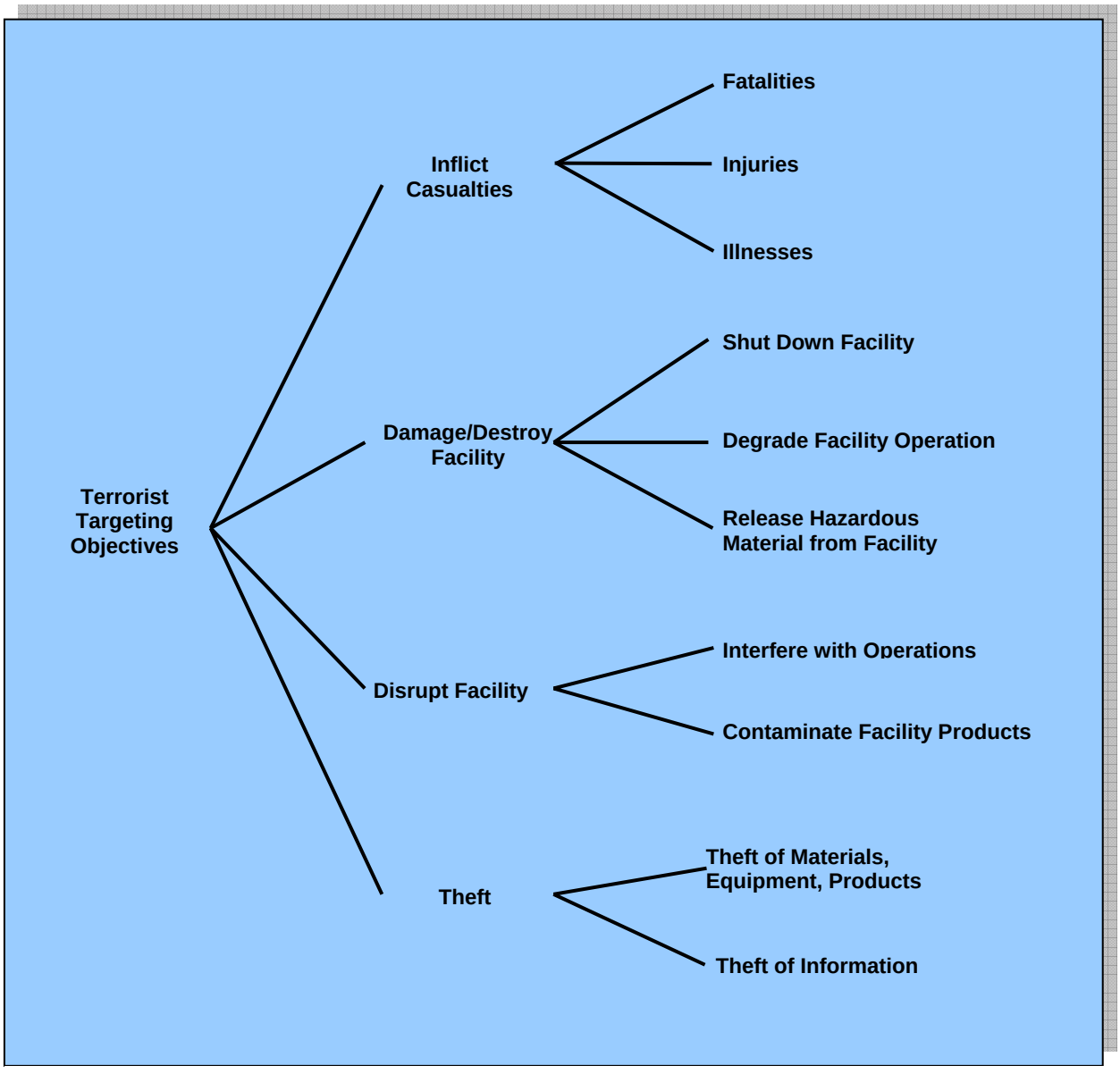

Figure 1 Potential Terrorist Targeting Objectives

FACILITY CHARACTERISTICS

The following sections provide a summary description of the hotel sector and some of the facility configurations that might be susceptible to terrorist threats.

Characterization of the Industry

In 2000, the American Hotel & 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, and 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	Comfort Inn, Quality Inn,	4,700	376

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)
International	Econo Lodge		
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.

Common Facility Characteristics and Vulnerabilities

Hotels are vulnerable because they must remain open, many people congregate there, there are numerous arrivals and departures, and there are many entrances and exits. 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 with vehicle parking beneath or within the structure may be more vulnerable to car bombs.

Figure 2 shows two types of atrium layouts—open-ended and enclosed. An atrium with open (rather than glass-walled) hallways along the atrium is more vulnerable to hazardous contaminants, including smoke, in the indoor air, than one with glass-enclosed hallways. This configuration is not especially vulnerable to structural damage from a bomb. Atrium-type structures are typically engineered for smoke control in the event of fire in the atrium. The smoke control system vents smoke upward from the atrium and keeps corridors and stairwells under positive pressure.

Figure 3 illustrates variations on a tower configuration with a central core. This type of structure has increased vulnerability to structural damage because utilities, elevators, stairways for emergency use, and backup systems are located in the central core. Tower configurations are not especially vulnerable to hazardous air pollutants because airflow can generally be compartmentalized.

The distribution of functional areas within a tower configuration is illustrated in Figure 4. Attacks on the integrity of the structure are likely to focus on the lower levels.

Various slab configurations for hotel structures are shown in Figure 5. These configurations allow for more separation of primary and backup systems. They also generally allow compartmentalization of airflow, limiting vulnerability to hazardous substances in the air.

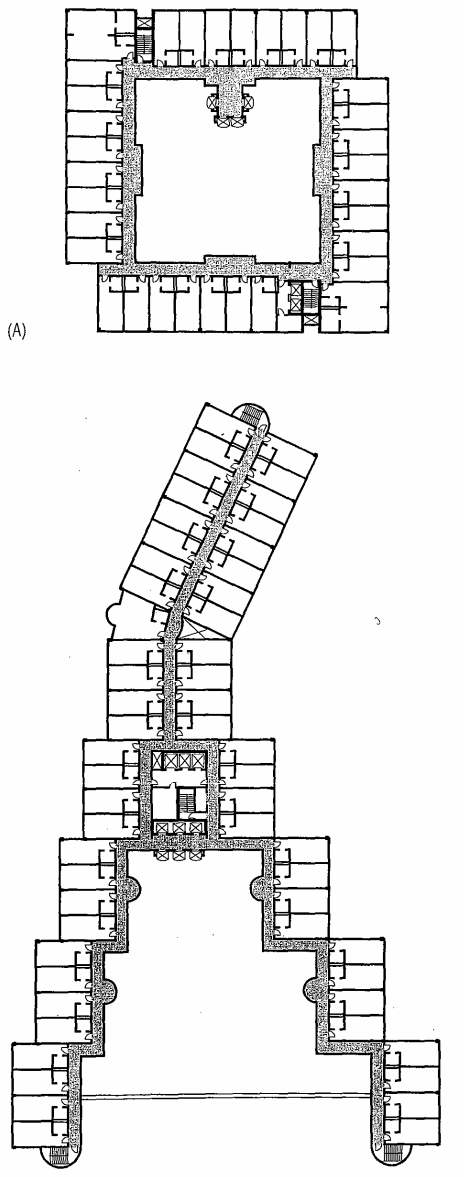

Figure 2 (a) Enclosed and (b) Open-ended Atrium Configurations (Source: Rutes et al., 2001)

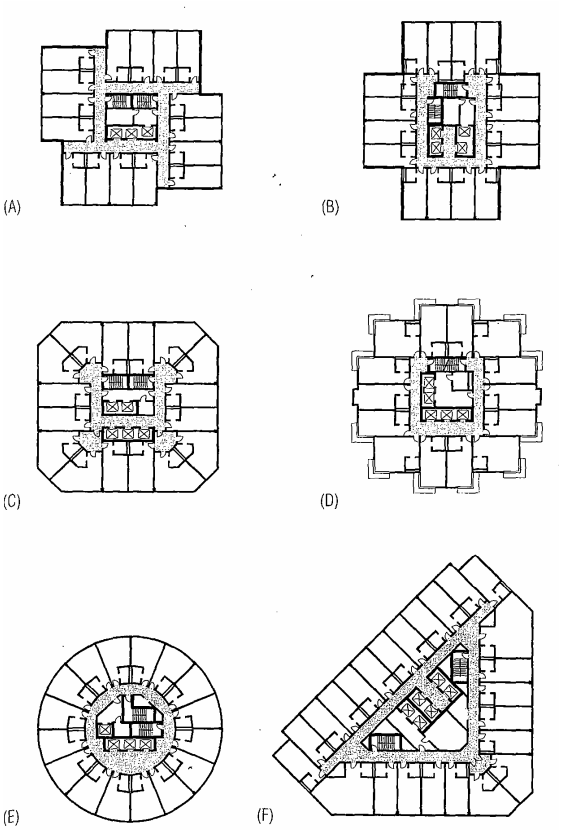

Figure 3 Tower Configurations with a Central Core (Source: Rutes et al., 2001)

The height of the structure can also affect hotel vulnerability; low-rise structures (one to two stories) are less vulnerable than high-rise structures. Structures with more than five stories may have greater issues with regard to patron evacuation in situations where elevators are unusable. Low-rise structures tend to be more dispersed and are generally less vulnerable to most types of threats for that reason. Figure 6 shows a dispersed facility design.

Hotels may also be integrated with other facilities, such as malls, casinos, convention centers, universities, and airports. Each of these situations carries site- and situation-specific vulnerabilities with it. Figure 7 shows the plan for a hotel integrated with an airport terminal. The hotel's atrium-style lobby is located over the main arrival and departure area of the airport. This proximity is likely to increase vulnerability of the hotel.

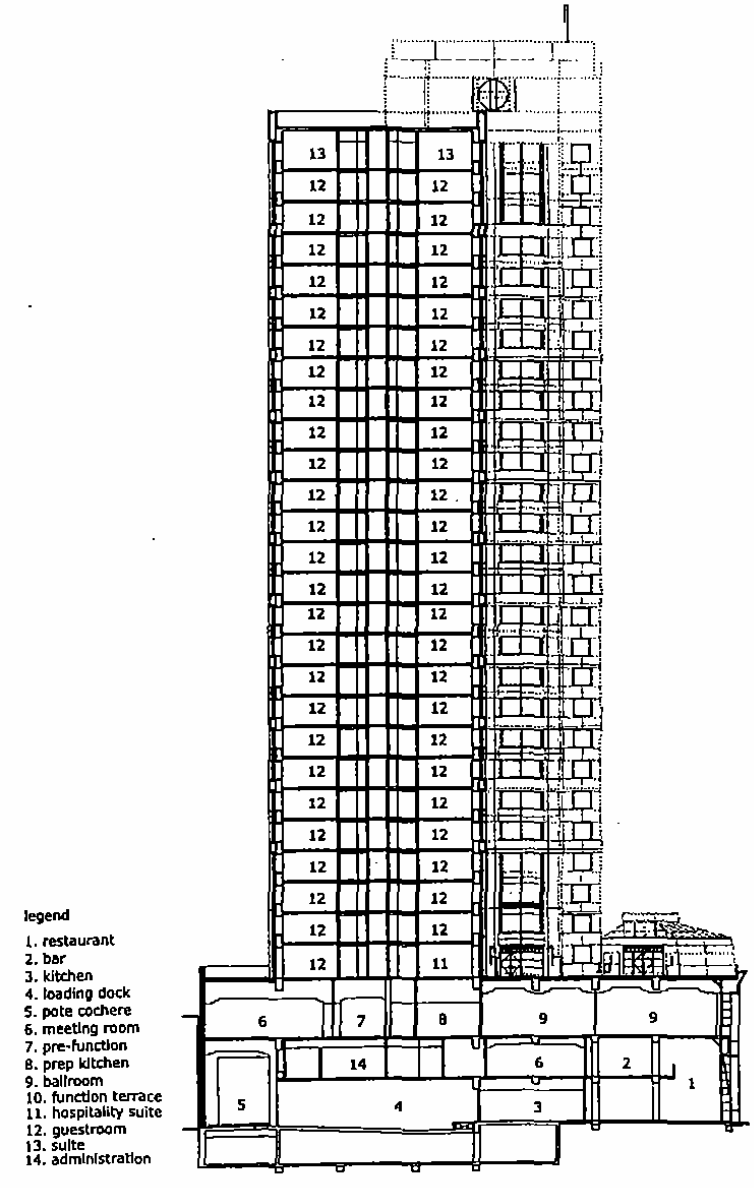

Figure 4 Arrangement of Functional Areas in a Tower Configuration (Source: Rutes et al., 2001)

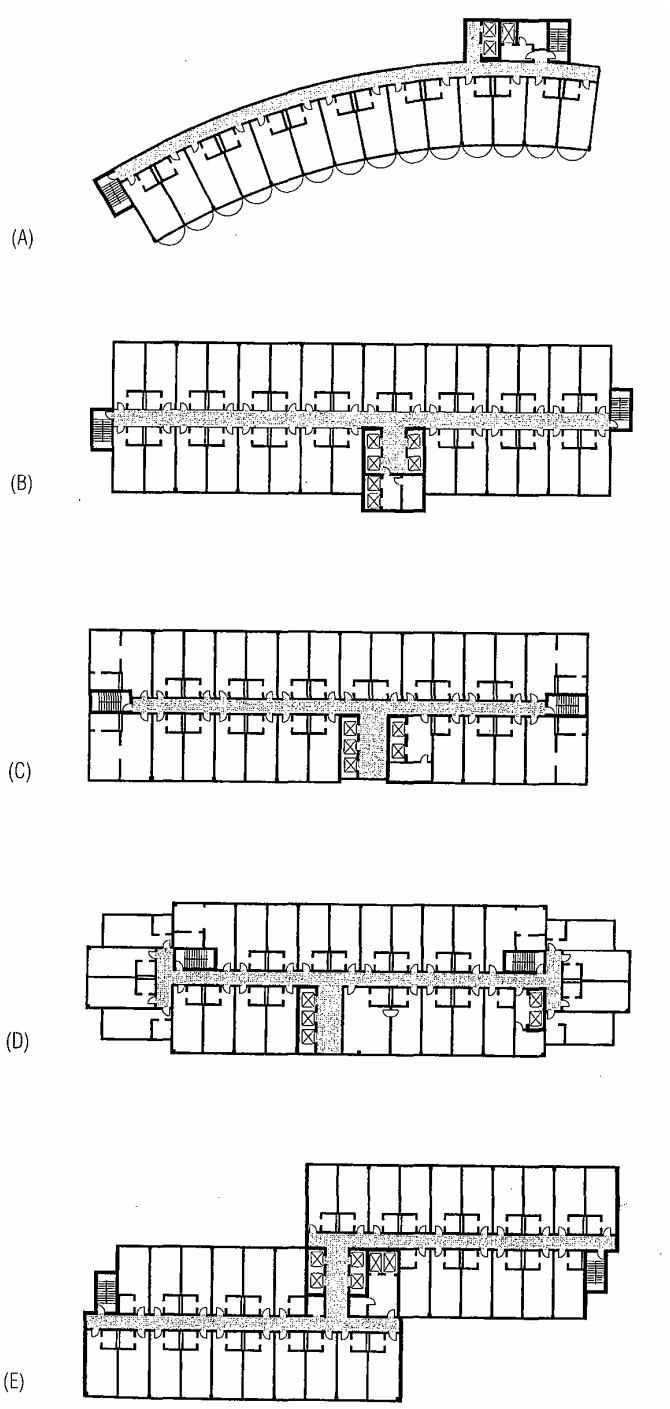

Figure 5 Slab Configurations for Hotel Structures (Source: Rutes et al., 2001)

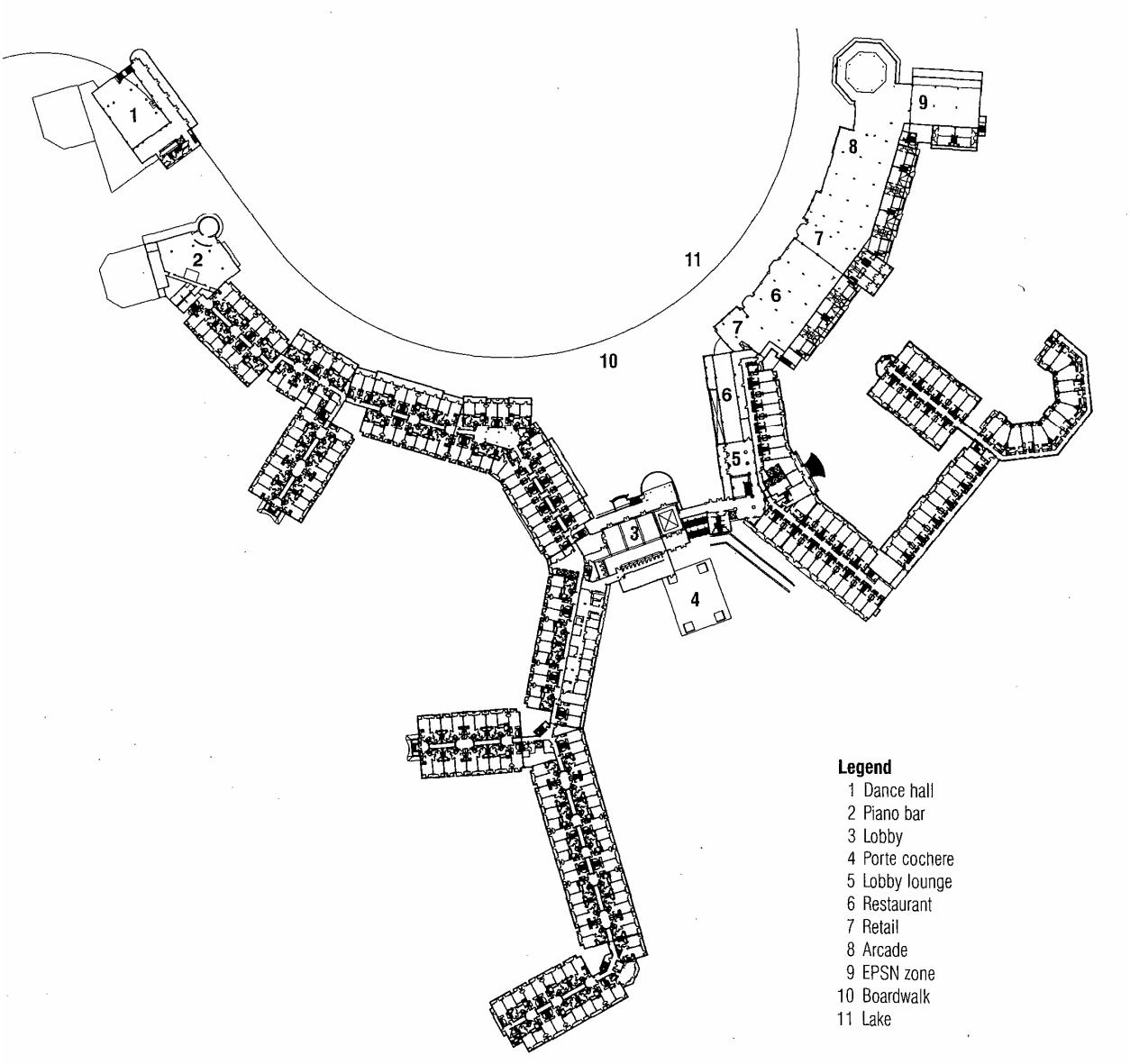

Figure 6 Dispersed Hotel Configuration (Source: Rutes et al., 2001)

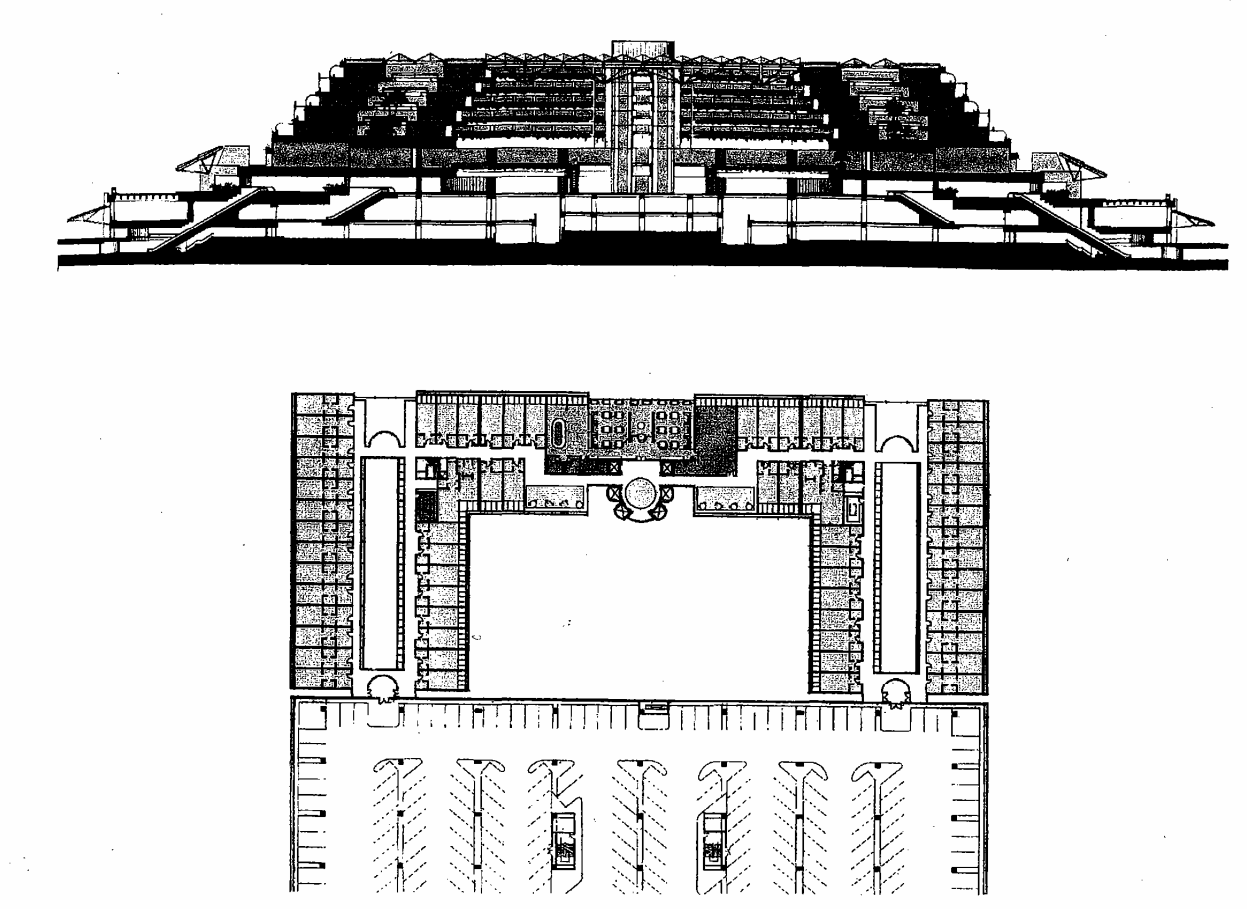

Figure 7 Integrated Airport Terminal Hotel (Source: Rutes et al., 2001)

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.

One of the key issues in hotel vulnerability to chemical, biological, and radiological attacks is the location and access control of the air intakes for the structure. As shown in Figure 8, higher intakes, especially those located in a sidewall, are least vulnerable. Figure 9 shows a relatively protected location (note: adjacent windows must be inoperable). Vulnerable air intakes can be modified to increase their security as shown in Figure 10.

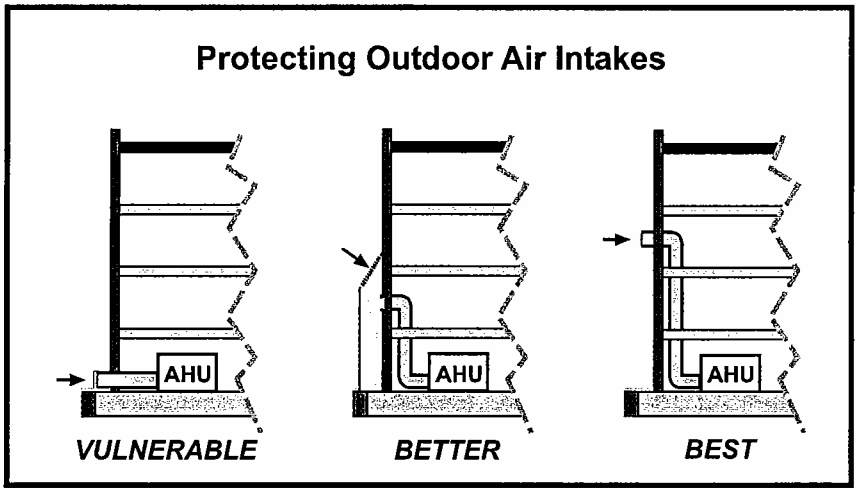

Figure 8 Vulnerability of Different Air Intake Locations (Source: NIOSH 2002)

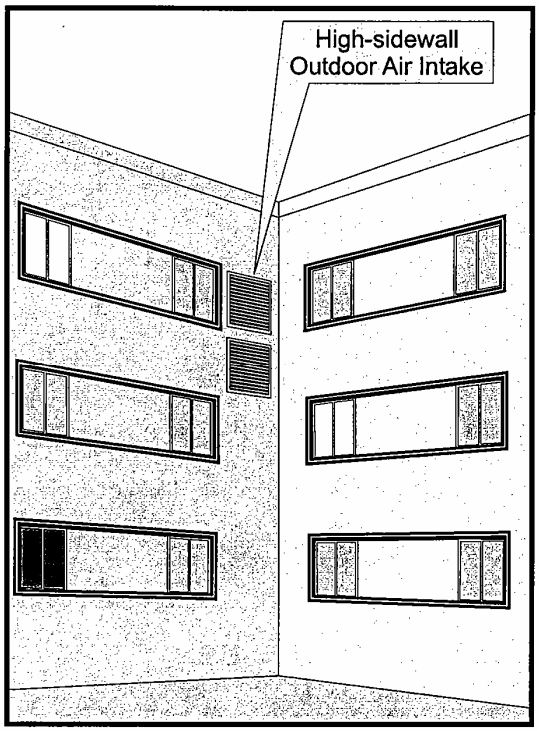

Figure 9 Protected Sidewall Location for an Air Intake (Source: NIOSH 2002)

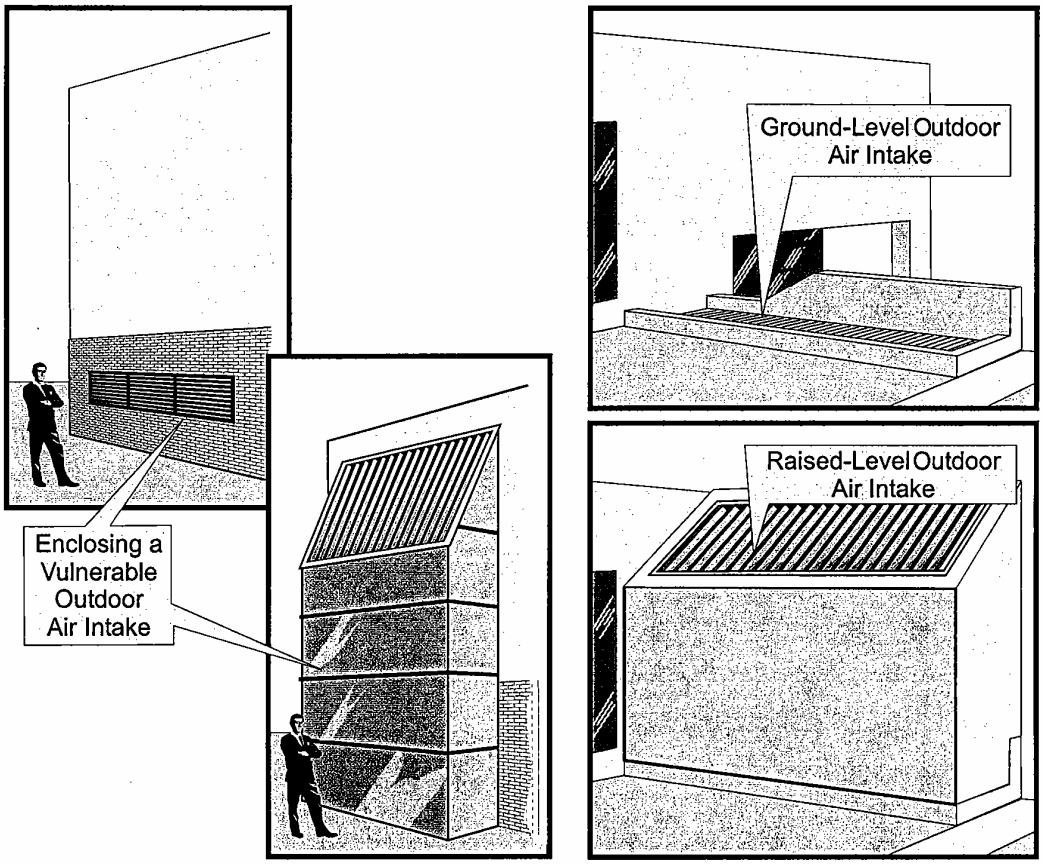

Figure 10 Modifications to Increase Security of Vulnerable Air Intake Structures (Source: NIOSH 2002)

Standards

Local building codes that apply to hotels generally address:

- Fire resistance of the structure,
- Compartmentalization of use areas,
- Flame spread,
- Fire resistance of furnishings,
- Fire detection alarms and fire suppression systems,
- Occupant load, and
- Exit requirements.

The National Fire Protection Association Life Safety Code applies to commercial buildings, including hotels.

The American Society of Heating, Refrigerating, and Air-Conditioning Engineers has issued guidance on managing risks to commercial buildings from biological, chemical, or radiological attacks. Some key points applicable to hotels include the following:

- Locate outdoor air intakes so that they are protected from contamination. Consider use of intrusion alarm sensors near the intakes.
- Control access to air distribution equipment and ductwork.
- Assure building envelope integrity, and maintain air pressure differentials across various functional zones of the building.
- Give fire protection the highest priority if there are conflicts with other strategies for terrorism protection.
- Include critical and life safety systems on standby power.
- Evaluate the need for air-cleaning filters and install filters with an appropriate efficiency level.
- Consider creating an area of refuge within the building, served by a separate air-handling system.
- Control building entries and exits.
- Install separate air-handling systems for the lobby, reception areas, and receiving docks to prevent the spread of contamination. Have a direct emergency exit to the outside.
- Develop an emergency response plan and drill employees.
- Install a public address system.

The Department of Homeland Security (http://www.ussecassoc.com/public/docs/hsbulletin.htm) has issued a set of recommended security procedures for owners of public access buildings to protect against vehicle bombs:

- 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.
- 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.
- Implement a counter-surveillance detection program.

CONSEQUENCE OF EVENT

An event has the potential to cause hundreds of injuries and possibly fatalities. Local emergency response agencies could incur extraordinary expenses for a response to a major attack on a large hotel (e.g., special collapsed building rescue) and may even experience death of or injury to emergency responders. Structural damage alone at a large, high-rise hotel could shut down operations for as long as a year, resulting in millions of dollars of economic damages for the hotel owner and for the local economy.

A devastating attack on a major U.S. hotel could result in public perception that hotels cannot be protected from a terrorist attack, which could have significant adverse economic effects on the lodging and tourism industry. Business and leisure users of hotel facilities might fear staying at a hotel or a particular chain of hotels that has been attacked. The loss of business and leisure travelers would ripple down to other commercial activities, such as restaurants, conventions, airlines, and entertainment that support the traveling public.

COMMON VULNERABILITIES

Critical infrastructures and key assets vary in many characteristics and practices relevant to specifying vulnerabilities. There is no universal list of vulnerabilities that applies to all assets of a particular type within an infrastructure category. Instead, a list of common vulnerabilities has been prepared, based on experience and observation. These vulnerabilities should be interpreted as possible vulnerabilities and not as applying to each and every individual facility or asset. Some hotels have instituted security vulnerability assessment protocols, site prioritization processes, and risk-based approaches to improving security performance, including provisions to increase security measures during heightened threat conditions. The security improvements implemented by hotels under such protocols may mitigate certain vulnerabilities listed below. The vulnerabilities list considers the issues within the physical perimeter boundaries of hotels. The majority of vulnerabilities that are inside hotels result from potential lack of access controls or structural configurations that are vulnerable to bombs.

Exhibit 1 Economic and Institutional Vulnerabilities	
Economic and institutional vulnerabilities are those that would have extensive national, regional, industry-wide consequences if exploited by a terrorist attack.	
1	A devastating attack on a major U.S. hotel could result in public perception that hotels cannot be protected from a terrorist attack, which could have significant adverse economic effects on the lodging and tourism industry.
2	An attack could have ripple effects on other commercial activities that support the traveling public.
3	A cyber attack could destroy all records of reservations and financial data causing significant economic losses and dissatisfied guests.

Exhibit 2 Site-Related Vulnerabilities	
Site-related vulnerabilities are conditions or situations existing at a particular site or facility that could be exploited by a terrorist or terrorist group to do economic, physical, or bodily harm or to disable or disrupt facility operations or other critical infrastructures.	
Access and Access Control	
1	Facilities may lack controlled access to air intakes for HVAC systems.
2	Facilities may lack controlled access to sprinkler control valves.
3	Facilities may lack protective barriers at the main entrance.
4	Exterior lighting may be inadequate.
5	Access to critical systems may not be adequately controlled.
6	Visitor parking areas may be adjacent to the facility.
7	Facilities may lack controlled access to the roof.
8	Facilities may lack controlled access of vehicles to parking areas located below and within the structure.
9	Facilities may lack controlled access of persons to special events within the hotel (e.g., bar mitzvah, fur garment sales, etc.)
10	Hotels are open to the public and many areas in the hotel are not restricted to guests with room keys (e.g., lobbies, convention/reception rooms, restaurants).
Design Issues	
11	Atriums present special vulnerabilities to fire and the introduction of hazardous/toxic substances.
12	Garages under hotels present vulnerabilities to vehicle-borne bombs.
13	Glass lobbies and entrances are difficult to protect from vehicle-borne bombs and stand-off weapons.
	(Continued on next page.)

Operational Security	
14	Technology for protection of HVAC systems is very limited, making access control critical. Ground-level air intakes are particularly vulnerable.
15	Background checks may not be conducted on all employees and contractors.
Emergency Planning and Preparedness	
16	Security functions may be understaffed.
17	Emergency plans may not be formalized or exercised and may not include response to terrorism events.
18	Many hotels use contract guard services, which may not be trained to respond to an intentional attack.
Hazardous and Toxic Chemicals	
19	Hazardous materials at hotels (e.g., chlorine for swimming pools) may not be adequately protected.
20	Ventilation systems could be vulnerable to introduction of hazardous or toxic chemicals or biological agents.
21	Hazardous chemicals could be used to start a fire or fires in key locations.
Other Hotel Operation Considerations	
22	Persons congregating at mealtimes and special events may present a target.
23	Contamination of food products.
Telecommunication	
24	Disruption of electrical service may also disrupt communications.
25	Staff may not have handheld, two-way communicators available to enable effective communication during an emergency.

Exhibit 3 Interdependent Vulnerabilities	
Interdependency is the relationship between two or more infrastructures by which the condition or functionality of each infrastructure is affected by the condition or functionality of the other(s). Interdependencies can be physical, geographic, logical, or information-based.	
General	
1	In hotels with high-rise tower configurations, emergency and backup systems may be located in the same central core as the primary utilities, making both vulnerable to the same structural damage.
2	Disruption of any or all utilities could disrupt operation of hotel services.
Natural Gas	
3	Natural gas service to the hotel could be interrupted causing loss of heating capability.
4	The natural gas supply system could be tampered with to create fire or explosions.
Water	
5	Water supply systems could be tampered with to inhibit fire-fighting capability.
6	Drinking water supplies could be contaminated.
7	Disrupted water supplies could create sanitation problems, which may necessitate evacuation of the building.
Electric Power	
8	Electric power service could be disrupted to create panic and inhibit evacuations.
9	Disruption of primary and backup electrical service could cause the interruption of fire and security alarm systems, telecommunications, elevator operations, HVAC operations, egress doors, garage entrances, and, often, the guest room door locks.
Telecommunication	
10	Disruption of electrical service may also disrupt communications.
11	Staff may not have hand-held, 2-way communicators available to enable effective communication during an emergency.
12	Disruption of phone service could cause interruption of fire and security systems ability to alert emergency personnel.
13	Disruption of phone service could impede the ability to directly contact emergency personnel.

USEFUL REFERENCE MATERIAL

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].

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

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.

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

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

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].

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

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

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

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].