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

Casinos

It is estimated that there are 648 casinos in the 31 states that allow legalized gambling. The term "casino" describes two types of facilities within the gaming industry that have their own unique characteristics but that are operationally quite similar: casino-hotels and non-hotel casinos. The latter category includes floating casinos.

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 casinos include the following:

- Improvised explosive devices
- Arson
- Chemical/biological/radiological agents
- Small arms 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., gambling areas, beverage or food courts) wearing unusually bulky clothing that might conceal suicide explosives; weapons (e.g., automatic rifle) may also be concealed under their clothing
- Unattended vehicles illegally parked near the casino entrance or places where large numbers of patrons gather
- Unattended packages (e.g., backpacks, briefcases, boxes) that might contain explosives
- Unauthorized access to heating, ventilation, and air conditioning (HVAC) areas; indications of unusual substances near air intakes

Indicators of potential surveillance by terrorists include the following:

- Persons discovered with a suspicious collection of casino/hotel maps, photographs, or diagrams with facilities highlighted
- Persons parking, standing, or loitering in the same area over a multiple-day period with no apparent reasonable explanation
- Persons using or carrying video/camera/observation equipment over an extended period
- Casino/hotel personnel being questioned off-site about practices pertaining to the casino
- Casino/hotel employees changing working behavior or working more irregular hours
- Persons observed or reported to be observing casino receipts or deliveries
- A noted pattern or series of false alarms requiring a response by law enforcement or emergency services
- Unfamiliar cleaning crews or other contract workers
- An increase in sensitive areas left unsecured
- An increase in threats from unidentified sources
- Unusual or unannounced maintenance activities in the vicinity of the casino/hotel
- Sudden losses or thefts of guard force or surveillance equipment
- Suspicious behavior of "patron" asking for and/or using safety deposit boxes

Common Vulnerabilities

The following are key common vulnerabilities of commercial casinos:

- Availability of large amounts of cash
- Unrestricted public access
- Large number of access points (to ground casinos)
- Congested patron gaming areas
- Unrestricted access to areas adjacent to buildings
- Limited employee background checks
- Unprotected HVAC systems and utility services
- Building designs that are not security oriented
- Multiple locations to place explosives or hazardous agents

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 casinos include the following:

- **Planning and Preparedness**
  - Develop a comprehensive security plan and emergency response plan based on threat analyses, vulnerability assessments, and consequence analyses
  - Conduct regular exercises of the plans
  - Develop policies and procedures for dealing with hoaxes and false alarms
  - Establish liaison and regular communication with local law enforcement and emergency responders
- **Personnel**
  - Conduct background checks on casino employees
  - Incorporate security awareness and appropriate response procedures for security situations into employee training programs
  - Maintain an adequately sized, equipped, and trained security force
- **Access Control**
  - Provide appropriate signs to restrict access to non-public and sensitive areas (e.g., surveillance rooms, hotel rooms, safety deposit area)
  - Identify and control access by all casino employees, vendors, delivery personnel, contractors, and patrons
  - Install and regularly test electronic access control systems and intrusion detection systems in sensitive areas
  - Identify key areas in or adjacent to the casino and control vehicle access/parking there
- **Barriers**
  - Provide adequate locks, gates, doors, and other barriers for designated security areas
  - Install and inspect blast-resistant trash containers
  - Install barriers at HVAC systems to prevent the introduction of chemical, biological, or radiological agents into the facility
  - Install active vehicle crash barriers at selected areas to protect buildings and populated areas
- **Communication and Notification**
  - Install, maintain, and regularly test the facility security and emergency communications system
  - Develop redundancy in the facility security and emergency communications system
  - Provide and periodically test redundant communication channels with local law enforcement and emergency responders
  - Take any threatening or malicious telephone call, facsimile, or bomb threat seriously
  - Provide a simple means for employees and patrons to report any situation or suspicious activity that might constitute a threat
- **Monitoring, Surveillance, Inspection**
  - Install closed-circuit television (CCTV) systems, intruder detection systems, and lighting to cover key areas
  - Train security personnel to watch for suspicious or unattended vehicles on or near facilities; repeated visitors or outsiders who have no apparent business in non-public areas of the casino; abandoned parcels, suitcases, backpacks, and packages and any unusual activities; and utility supplies and routine work activities scheduled on or near assets
  - Regularly inspect lockers, mail room areas, hotel area, trash bins, parking lots and garages, and all designated security areas under access control
- **Cyber Security**
  - Implement, review, and regularly test hardware, software, and communications security for computer-based operational systems
- **Infrastructure Interdependencies**
  - Provide adequate capacity, redundancy, security, and backup for critical utility services (e.g., electricity, natural gas, water, telecommunications) for normal and emergency needs
  - Provide for regular monitoring and inspection of utility services (e.g., security force patrols, CCTV) and testing of backup capability
- **Incident Response**
  - Identify emergency entry and exit points to be used in emergencies and regularly inspect them

More detailed information on casinos is contained in the document, *Casinos: Potential Indicators of Terrorist Activity, Common Vulnerabilities, and 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 listed below.

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