U.S. Department of Homeland Security
Protective Security Coordination Division
Office of Infrastructure Protection

Infrastructure Protection Report Series

Executive Summary - Shopping Malls

The United States has more than 46,000 shopping malls nationwide, ranging in size from small open-air neighborhood “strip” shopping centers containing fewer than 10,000 square feet (ft^2) of store area to super-regional malls with more than 1 million ft^2.

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 shopping malls may include:

- Complex Terror Attack
- Active Shooter and Small Arms Attack
- Improvised Explosive Device
- Vehicle-Born Improvised Explosive Device (VBIED)
- Arson
- Insider Threat

Terrorist activity indicators are observable anomalies or incidents that may precede a terrorist attack. Indicators of an potential attack requiring action may include the following observed behaviors or incidents occurring in or around the mall and surrounding community:

- Suspicious persons in crowded areas wearing unusually bulky clothing that might conceal explosives; potential getaway vehicles staged in or near a mall parking lot
- Unexpected or unfamiliar delivery trucks arriving at the facility
- Unattended or suspicious packages (e.g., backpacks, briefcases, boxes) and/or letters received by mail
- Recent damage or vandalism (e.g., significant holes or cuts) to non-public areas, perimeter lighting, or other security devices (e.g., damage to video cameras, locks, doors, or security gates)

Indicators of potential surveillance by terrorists include:

- Persons using or carrying video/camera/observation equipment or night vision devices in or near the facility over an extended period
- Persons parking, standing, or loitering in the same area over a multiple-day period with no apparent reasonable explanation
- Persons excessively inquiring about practices pertaining to the facility and its operations or the facility’s supporting (telecommunications, electricity, natural gas, water) infrastructure
- Persons observed or reported to be observing facility receipts or deliveries
- Employees observed or reported to be willfully associating with suspicious individuals, changing working behavior, or working more or irregular hours

Common Vulnerabilities

The following are key common vulnerabilities of shopping malls:

- Open Access
- Building Design
- Security Force
- Lack of Coordination for and Dissemination of Emergency Plans
- Staff Turnover and Limited Employee Background Checks
- Natural and Other Hazards

Protective Measures

Recommended improvements in all-hazards protection and resilience planning for shopping malls include: equipment, personnel, procedures, information sharing, and cybersecurity elements designed to protect a facility against threats, mitigate the effects of an incident, and recover from an incident. Potential baseline protective and resilience measures for shopping malls include:

- **Equipment**
  - Install video surveillance systems and lighting to cover key areas (e.g., all entrances, exits, elevator lobbies, restrooms, public spaces, and all access points to HVAC equipment)

  - Provide appropriate signage indicating restricted access to non-public areas
  - Provide adequate locks, gates, doors, and other barriers for designated security areas
  - Install decorative bollards or crash barriers around selected areas to protect buildings and populated areas from blast effects (e.g., to protect against VBIEDs)
  - Install, maintain, and regularly test a facility security and emergency communications system
  - Provide adequate security and backup for critical utility services (e.g., electricity, natural gas, water, and telecommunications)
  - Locate fuel storage tanks at least 100 feet from all mall buildings and customer congregation points
  - Inspect and consider blast-resistant or blast-mitigating features for windows and trash containers

- **Personnel**
  - Consider conducting background checks for all mall management staff and security personnel
  - Incorporate security awareness and appropriate response procedures for security situations into mall and mall tenant employee orientation or training programs
  - Increase visibility of uniformed security personnel to deter possible unwanted activity
  - Identify and control non-public access points for all mall and mall tenant employees, vendors, delivery personnel, and contractors
  - Train security personnel to watch for suspicious or unattended vehicles; repeated visitors with no apparent business in non-public areas of the mall; abandoned parcels, backpacks, and packages; and unusual activities
  - Encourage employees and the public to report anything that appears to be odd or suspicious

- **Procedures**
  - Identify key areas in or adjacent to mall buildings, and prohibit parking in these areas
  - Implement ID checks and routinely enforce ID requirements for anyone in areas that are not open to the public
  - Regularly inspect lockers, mail room areas, trash bins, parking lots and garages, and all designated security areas under access control
  - Verify questionable deliveries and contractors with the mall employee or mall tenant who made the order
  - Develop a comprehensive security plan and emergency response plan in coordination with local law enforcement and emergency responders; Develop a plan to evacuate employees and shoppers out of the building during a major incident when warranted
  - Conduct regular exercises (e.g., tabletop exercises) of security and emergency response plans with local law enforcement and fire department officials
  - Develop policies and procedures for responding to hoaxes and false alarms
  - Develop policies and procedures for communicating with the media and the general public in the event of an incident to advise them of the situation and to defuse rumors and panic
  - Identify entry and exit points to be used in emergencies that are free of obstructions and can be fully utilized. Identify alternate rallying points where employees can gather for coordinated evacuation

- **Information Sharing**
  - Engage in routine security-focused communication with management of integrated facilities, local law enforcement, and emergency responders

- **Cyber Security**
  - Implement and review hardware, software, and communications security for computer-based operational systems
  - Require employees to use a specific login and unique password to access their electronic files
  - Eliminate information from mall Web site that might aid potential adversaries in planning an attack

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:
PSCD Operations
(PSCDOperations@hq.dhs.gov).