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

Large Residential Buildings

Large residential, or multifamily, buildings include apartments, condominiums, and cooperatives. These are generally high-rise structures that are characterized by controlled-access lobbies, common areas (e.g., meeting rooms, exercise rooms), on-site parking, and a staff to maintain the common areas and grounds of the building. There are more than 19 million housing units in residential structures with 5 or more units. Of these, more than 4 million units are in buildings with 50 or more units.

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 large residential buildings include:

- Improvised explosive devices or vehicles
- Arson
- Chemical/biological/radiological (CBR) agents
- Small arms attack or suicide bombers

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 (employees, guests, contractors, vendors, tenants) in a building wearing unusually bulky clothing that might conceal suicide explosives or weapons (e.g., gun, automatic rifle)
- Unattended vehicles parked illegally or at the parking area or near the building entrance for no apparent reasonable explanation
- Unattended packages (e.g., backpacks, briefcases, boxes) that might contain explosives
- Unauthorized access to restricted areas, especially the heating, ventilation, and air-conditioning (HVAC) system; indications of unusual substances near air intakes or exhaust

Indicators of potential surveillance by terrorists include:

- Persons discovered with building photos or diagrams with the detailed layout highlighted
- Persons parking, standing, or loitering in the same area for many days with no apparent reasonable explanation
- Persons using or carrying video/camera/observation equipment over an extended period
- Residential building employees or occupants being questioned off site about security practices that pertain to the building or the location of surveillance equipment
- Building employees changing their working behavior or working more irregular hours
- Persons noticed or reported to be observing building security, HVAC system, delivery, or storage areas
- A noted pattern or series of false alarms requiring a response by law enforcement or emergency services
- Unfamiliar employees (e.g., cleaning crews) or other contract workers
- Unusual or unannounced repair or maintenance activities near the building
- Sudden losses or thefts of building surveillance equipment

Common Vulnerabilities

The following are key common vulnerabilities of large residential buildings.

- Inadequate control of access to the building by nontenants and their vehicles (at exterior doors, doors to adjacent public transit stations, utility tunnels, loading docks, parking garages)
- The design of a building and materials used to construct it, which might enhance the probability that it would be damaged in an attack
- Inadequate protection of the HVAC system
- Inadequate protection of the utility services (electricity, natural gas, water, communications)
- Inadequate emergency response preparations
- Inadequate control of access to sensitive building information

Version September 13, 2006

Protective Measures

Protective measures include equipment, personnel, and procedures designed to protect a residential building against threats and to mitigate the effects of an attack. Protective measures for large residential buildings include:

- **Planning and Preparedness**
  - Develop a comprehensive security plan and emergency response plan (for tenants, employees, guests, contractors) to prepare for and respond to emergency situations, including malicious or terrorist actions.
  - Conduct regular exercises of the plans.
  - Maintain a constant awareness of the current threat condition and available intelligence information.
  - Develop policies and procedures for dealing with hoaxes and false alarms.
- **Personnel**
  - Conduct background checks on building employees (management, service, maintenance, security guards).
  - Incorporate security awareness and appropriate response procedures for emergency situations in training programs for building tenants and employees.
- **Access Control**
  - Deny access to any nontenant who displays suspicious behavior.
  - Identify and control access by employees, tenants, guests, vendors, delivery personnel, and contractors.
  - Remove any vehicles that have been parked for an unusual length of time at or near the building.
- **Barriers**
  - Provide adequate locks, doors, and other barriers for designated areas (elevators; HVAC system, storage, delivery, and utility areas; mechanical rooms; roof).
  - To the extent practical, minimize the number of places in public areas where an intruder could remain unseen or that could be used to hide weapons.
  - Provide adequate exterior lighting, including emergency lighting, where appropriate, to help in detecting suspicious or unusual activity.
- **Communications and Notification**
  - Install, maintain, and regularly test the building security and emergency communications system.
  - Communicate information on the threat level to tenants, employees, and security force; encourage tenants and employees to report any threat or suspicious situation.
  - Take any threatening or malicious telephone call, fax, or bomb threat seriously.
- **Monitoring, Surveillance, Inspection**
  - Install closed-circuit television (CCTV) systems, entrance metal detectors (if practical), intruder detection systems, and lights to cover key areas (entrances; exits; parking lots; hallways; roof; HVAC, utility system, delivery, mail, and storage areas).
  - Monitor contractors and delivery personnel while they are on the premises. Restrict the type of personal items that employees, contractors, vendors, and guests can bring to nonpublic areas of the building.
  - Train security personnel to watch for suspicious persons and unattended vehicles in or near the building; abandoned parcels, suitcases, backpacks, and packages; and unusual activities; and to monitor all deliveries to the building.
  - Regularly inspect and monitor restricted areas, trash bins, utility and storage areas, parking lots, the roof, mechanical rooms, and HVAC systems.
- **Infrastructure Interdependencies**
  - Provide adequate security and backup for critical utility services (e.g., electricity, natural gas, water, sewer, communications).
- **Cyber Security**
  - Implement and review, if applicable, computer-based operational systems.
  - Eliminate any information that might be useful to adversaries from the building Web site.
- **Incident Response**
  - Maintain an up-to-date emergency response plan.
  - Alert appropriate law enforcement and public health authorities to any evidence of tampering with the HVAC system or water or gas supply or of other malicious, criminal, or terrorist activities.

More detailed information on large residential buildings is contained in the document, *Large Residential Buildings Potential Indicators of Terrorist Activity, Common Vulnerabilities, and Protective Measures*, which is available from the contacts below.

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