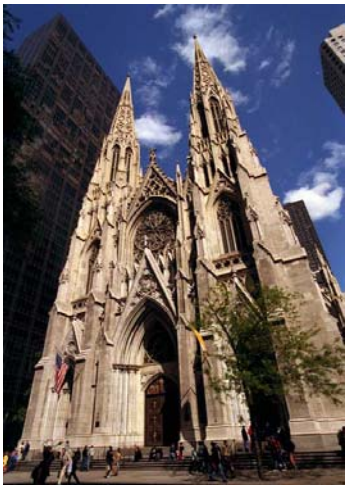
U.S. Department of Homeland Security
Protective Security Coordination Division
Office of Infrastructure Protection

Infrastructure Protection Report Series

Religious Facilities

Hundreds of thousands of religious facilities serve millions of people of all faiths and denominations throughout the United States. Religious facilities are generally open-access public assembly venues and have been successfully targeted by terrorists on numerous occasions in the past.



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 religious facilities include:

- Improvised explosive devices (IEDs)
- Arson/ incendiary attack
- Small arms attack
- Assassination/kidnapping
- 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., reception or meeting areas) wearing unusually bulky clothing that might conceal suicide explosives or weapons
- Suspicious or illegally parked vehicles near facility or near places where crowds gather
- Unattended packages (e.g., backpacks, briefcases, boxes) that might contain explosives
- Suspicious package or letter received by mail that might contain explosives or chemical, biological, or radiological agent
- Unexpected or unfamiliar delivery or maintenance vehicles
- Evidence of unauthorized access to areas of the building containing heating, ventilation, and air-conditioning (HVAC) equipment

Indicators of potential surveillance by terrorists include:

- Persons using or carrying video/camera/observation equipment in or near the facility over an extended period
- Persons discovered with facility maps, photos, or diagrams with critical assets highlighted or listing of personnel
- Persons questioning religious facility employees off-site about practices pertaining to the facility and its operations
- Persons parking, standing, or loitering in the same area over a multiple-day period with no reasonable explanation
- Facility employees associating with suspicious individuals
- An increase in threats from unidentified sources by telephone, postal mail, or e-mail and/or an increase in reports of threats from outside known, reliable sources

Common Vulnerabilities

The following are key common vulnerabilities of religious facilities:

- Significant numbers of people of like faith gathered in a single symbolic location at specified times
- Generally unrestricted access to religious services
- Unrestricted access to peripheral areas, such as contiguous parking areas and separate educational facilities
- Building systems that are vulnerable to fire, contamination via heating and cooling systems, explosives, and blocked emergency exits
- Access by workers and maintenance staff who may not undergo background checks
- Easy facility identification either by facility configuration, design, or signage
- Non-profit status, which may result in limited resources for security

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 religious facilities include:

- **Planning and Preparedness**
  - Designate an employee as security director
  - Develop a comprehensive security plan and emergency response plan for the facility
  - Establish liaison and regular communication with local law enforcement and emergency responders
  - Conduct regular exercises with facility employees to test the security and emergency response plans
- **Personnel**
  - Conduct background checks on all employees
  - Incorporate security awareness into employee training programs
  - Maintain an adequate security force using both employees and congregation volunteers
- **Access Control**
  - Define the facility perimeter and areas within the facility that require access control
  - Limit access to congregation members and visitors to a level consistent with facility operations
  - Keep vehicles away from critical assets and from areas where large numbers of people congregate
  - Require that all illegally parked vehicles be moved or have them towed
  - Provide adequate door and window locks, barred entryways, and fencing and gate locks to areas where access is to be limited; add intrusion detection systems and alarms as appropriate
  - Train mail room and receiving personnel to recognize suspicious mail, packages, shipments, or deliveries
- **Barriers**
  - Evaluate the need for perimeter barriers (e.g., fences, berms, concrete walls) around the facility
  - Establish a clear zone adjacent to sensitive or critical buildings; keep zone free of vegetation and other obstructions to allow for continuous monitoring
  - Install barriers to protect doors and windows from small arms fire and explosive blast effects
  - Install barriers at HVAC systems to prevent the introduction of chemical, biological, or radiological agents into the building
- **Communication and Notification**
  - Install system(s) that provide communication with all individuals at the facility, including employees, security force personnel, congregation members, and visitors
  - Develop a notification protocol that specifies who should be contacted in emergencies
- **Monitoring, Surveillance, Inspection**
  - Evaluate needs and design a monitoring, surveillance, and inspection program that is consistent with facility operations and security requirements
  - Provide visual surveillance capability for sensitive and critical assets at the facility
  - Continuously monitor all people entering and leaving the facility; train monitors to detect suspicious behavior
- **Infrastructure Interdependencies**
  - Ensure that the facility has adequate utility service capacity to meet normal and emergency needs
  - Secure dumpsters and other trash containers to prevent the hiding of explosives or other hazardous materials
- **Cyber Security**
  - Develop and implement a security plan for computer and information systems hardware and software
  - Design and implement a secure computer network architecture
  - Regularly review facility Web site to ensure that no sensitive information is provided
- **Incident Response**
  - Ensure that an adequate number of emergency response personnel are available at all times
  - Check the status of all emergency response equipment and supplies on a regular basis
  - Identify entry and exit points to be used in emergencies
  - Ensure that employees are familiar with procedures for shutting off utility services (e.g., electricity, natural gas) in emergency situations