1 Background

The United States has approximately 345,000 religious congregations consisting of about 150 million members. These members comprise more than 230 different denominational groups (Grammich *et al.* 2012). The number of people coming and going from religious facilities during the week varies with the size of the congregation living nearby. In rural areas, congregations are generally small (100 members or less). In large metropolitan areas and suburbs, congregations can exceed 10,000 members. Some religious facilities also provide educational resources for students in prekindergarten and kindergarten through 12th grade. Some religious facilities, like the Washington National Cathedral, are national icons.

1.1 Deliberate Attacks

Religious facilities can be attacked using a variety of different methods, including active shooters; improvised explosive devices (IEDs); vehicle-borne improvised explosive devices (VBIEDs); chemical, biological, or radiological attacks; and arson.

1.2 Natural Hazards/Accidents

Religious facilities can be adversely affected by a variety of natural hazards, e.g., infectious diseases and illnesses, fire, and seismic and weather-related events (hurricanes, tornadoes, flash floods). Such hazards can affect the safety of religious facilities' employees and members, as well as the facility's ability to carry out normal operations.

Wooden Church After Tornado Damage
Source: Shutterstock

Taken together the sheer number of religious facilities in the United States, the scheduling and predictability of times when members gather to worship (which facilitate surveillance and targeting), and the attractiveness of religious facilities as a "soft target," lead to the following industry-wide security- and protection-related challenges:

- **Prevention of attacks.** Religious facilities and their members have been targets of violent attacks. These incidents have served to point out vulnerabilities and have offered valuable lessons for protecting these facilities, the people who attend them, and the employees who work in them.
- **Natural disaster/mass casualty events**. Effective planning and preparedness training for potential natural disasters and other mass casualty events enables religious facilities personnel to identify their roles in evacuation and/or relief efforts that may be necessary in the event of an unforeseen catastrophe.

2 Potential Threats and Attack Indicators

Potential threats to religious facilities can originate from disaffected individuals, e.g., employees, or outsiders, and domestic and international terrorist groups. According to statistics compiled by the U.S. Department of Justice (DOJ), approximately 19% of all hate crimes recorded in 2009 were directed at were directed at individuals because of a bias against a religious belief (DOJ 2009). Natural hazards can affect religious facilities directly, e.g., a tornado that does significant damage to a place of worship, or indirectly, by adversely affecting upstream suppliers, e.g., electricity, and thus disrupting the supply chain. Therefore, a comprehensive strategy is required that combines risk-informed prevention, protection, and preparedness activities with resilience enhancements to manage and reduce the most serious risks these facilities face.

2.1 Threats

Adversaries have a wide variety of weapons and tactics available to achieve their objectives and have demonstrated the ability to plan and conduct complex attacks against multiple targets. Attacks can be carried out by individuals, small teams of a few perpetrators, or larger groups acting in a coordinated fashion. Specific threats of most concern to religious facilities include the following:

2.1.1 Active Shooter and Small Arms Attack

These attacks can be launched using conventional firearms, automatic weapons, shoulder-launched rocket-propelled grenades, explosives, or similar weapons to indiscriminately shoot people or take hostages.

2.1.2 Improvised Explosive Device

An IED or “homemade bomb” can be constructed of commonly available materials, construction explosives (e.g., dynamite), or stolen military-grade explosives. An IED can be carried into a religious facility by an individual (e.g., a suicide bomber) or can be deposited in an unnoticed location for detonation by a timer or by remote control.

2.1.3 Vehicle-Borne Improvised Explosive Device

Religious facilities are also vulnerable to VBIED attacks – IEDs loaded into a vehicle (car, truck, or motorcycle). The vehicles can be parked close to a religious facility and placed where large numbers of people gather, or they can be crashed through barriers and detonated. They are much larger and more dangerous than IEDs carried by an individual.

2.1.4 Arson

Intentional fires can be set by igniting highly flammable materials (e.g., gasoline) at a religious facility. Accelerants that promote the spread and intensity of a fire can be applied beforehand and then ignited.

2.1.5 Assassination and Kidnapping

Many terrorist acts have involved the assassination of key personnel or the kidnapping of individuals and hostage-taking.

2.1.6 Chemical, Biological, or Radiological Attack

Chemicals that can be used as weapons include toxic industrial chemicals (e.g., ammonia, hydrogen fluoride, chlorine) that are brought near or into a religious facility where they are dispersed by explosives, and chemical warfare agents (e.g., sarin, VX). Although the latter are not readily available, they have been procured and used by terrorists. Biological pathogens (e.g., anthrax, botulin, plague) can be introduced into a facility through its heating, ventilation, and air-conditioning (HVAC) system; or can be spread by contact (e.g., through contaminated letters delivered by mail).

2.2 Potential Indicators of an Attack[1]

Attack indicators are observable anomalies or incidents that may precede an attack or be associated with surveillance, training, planning, preparation, or mobilization activities. Potential indicators can be grouped into the following categories: imminent attack indicators, surveillance indicators, and surrounding area indicators.

2.2.1 Imminent Attack Indicators

These indicators may show that an attack is imminent and that immediate action needs to be taken. Indicators of an imminent attack include people, vehicles, or packages that demonstrate unusual or suspicious behavior that requires an immediate response. Potential indicators of an imminent attack are listed in Table 1.

2.2.2 Surveillance Indicators

Surveillance indicators may provide evidence that a religious facility is under surveillance by individuals planning an attack. Indicators of potential surveillance include persons in the vicinity of religious facilities intending to gather information about the facility or its operations and protective measures. Potential indicators that religious facilities may be under surveillance are listed in Table 1.

2.2.3 Surrounding Area Indicators

Surrounding area indicators relate to activities in the area or region surrounding religious facilities and may demonstrate that an attack is being prepared. In addition to indicators that might appear at religious facilities themselves, there are indicators that may appear in the communities surrounding religious facilities that should be considered and factored into decisions regarding security. These indicators are generally identified by local law enforcement. Religious facilities can establish communication channels with these organizations to maintain awareness of potentially threatening situations in the area and to piece together information from their facility with information from the surrounding area.

[1] Indicators identifies in this section are based primarily on information found in U.S. Department of Homeland Security (DHS) (2007) and New Jersey Office Of Homeland Security & Preparedness (NJOHSP) (n.d.), as well as information gathered during site visits to critical infrastructure sites as part of the Enhanced Critical Infrastructure Program.

Table 1: Potential Indicators of an Attack

Imminent Attack Indicators
• Suspicious persons in crowded areas wearing unusually bulky clothing that might conceal explosives. • Unexpected or unfamiliar delivery trucks arriving at the facility. • Unattended packages (e.g., backpacks, briefcases, boxes) or suspicious packages and/or letters received by mail. • Recent damage (e.g., significant holes or cuts) to a perimeter fence or gate, perimeter lighting, or other security devices.
Surveillance Indicators – Suspicious Persons
• 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 infrastructure (telecommunications, electric, natural gas, water). • 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 irregular hours.
Surveillance Indicators – Suspicious Activities Observed or Reported
• An increase in buildings left unsecured or doors left unlocked, when they are normally secured and locked at all times. • A noted pattern of false alarms requiring a response by law enforcement or emergency services. • Theft of employee or contractor identification cards, uniforms, or guard force communications equipment or unauthorized persons in possession of facility ID cards, uniforms, or equipment. • Unfamiliar contract workers attempting to access unauthorized areas. • Unusual and unexpected maintenance activities (e.g., road repairs) near the facility. • Sudden increases in power outages designed to test the backup systems or recovery times.

3 Common Vulnerabilities and Protective Measures[2]

This section identifies key common vulnerabilities associated with religious facilities and corresponding protective measures that can be adopted to address those vulnerabilities. While not all of these potential vulnerabilities are applicable to all religious facilities, they have been identified as priority focus areas for religious facilities management and security personnel to review.

3.1 Vulnerabilities

3.1.1 Open Access

- **Unrestricted access to religious services**. In general, religious facilities are open to all, at least during the conduct of religious services. Depending on the type of structure, the nature of access restrictions and other security measures that may be in place, religious facilities may or may not be able to control access to the facility by potential adversaries. Some high-risk facilities employ private security guards and/or local police to assist in access control.
- **Unrestricted access to peripheral areas**. Religious facilities are vulnerable to attacks outside their main building, such as in contiguous parking areas, where vehicles have unrestricted access and are generally not inspected, and in auxiliary buildings such as educational facilities.
- **Proximity of religious facilities and neighboring facilities, especially in urban areas**. Many religious facilities are located in urban areas in close proximity to homes and small businesses. This

[2] Material in this section is based, in large part, on Federal Emergency Management Agency (FEMA) (2005, 2011, 2012).

can make it more difficult to maintain effective perimeter security.

- **Limited or no vehicle access controls**. The layouts of most religious facilities permit close proximity of vehicles to buildings and areas where people congregate. These include parking areas, driveways on facility grounds, and nearby streets. There are usually no vehicle barriers near the main entrances or other vulnerable parts of the buildings.
- **Lack of control of vendor and contractor personnel**. Individuals who deliver parcels or are hired to do construction or repair work are often given unescorted access to religious facilities, and the contents of packages they deliver or materials brought into the facility are not inspected.
- **Unprotected utilities.** Religious facilities are generally not secured, leaving HVAC units and other critical building utility supply components (e.g., water, electric power, natural gas service) easily accessible.

St. Patrick Catholic Church, San Francisco, CA
(Source: Stock Photo)

3.1.2 Gathering of People of a Particular Faith

A religious facility attracts a group of people of like faith into a single location at specified times. This makes the facility a ready target for an adversary seeking to attack that particular group of people. This vulnerability is increased by easy identification of the specific faith, either by facility configuration or signage.

3.1.3 Limited Security Budget

Most religious facilities are nonprofit. Many have very small budgets that are used to pay for the basic operation of the facility and to provide services to the congregation and surrounding communities. Many do not have the financial resources to implement extensive security measures. Thus, for example, workers and volunteers may not undergo background checks.

3.1.4 Natural and Other Hazards

Many natural and other hazards can affect the safety of religious facilities, as well as the religious facility's ability to carry out normal operations. A religious facility's emergency action plans, security plans, and business continuity plans can provide the basis for responding to unexpected or catastrophic events. When evaluating these types of plans, potential or probable scenarios based on the religious facility's geographic location should be considered. The hazards most common to religious facilities include tornadoes, floods, and hurricanes.[3]

3.2 Protective Measures

Protective measures include equipment, personnel, and procedures designed to protect a facility against threats and to mitigate the effects of an adverse event. Many different protective measures are available for deployment at a facility and in the areas surrounding a facility (buffer zones). Some are applicable to a wide range of facilities and against a number of threat streams, while others are designed to meet the unique needs of a specific facility or a specific threat stream. In addition, some may be tactical in nature, while others may address long-term strategic needs (e.g., redundancy). Some protective measures are

[3] For more information on hazards and FEMA guidelines, see FEMA (2009).

designed to be implemented on a permanent basis to serve as routine protection for a facility. Such measures are sometimes referred to as "baseline countermeasures." Others are either implemented or increased in their application only during times of heightened alert.

The relatively open access to religious facilities building and grounds makes it difficult to secure religious facilities. Protective measures should be comprehensive, integrating equipment, personnel, procedures, and information sharing to ensure that all employees and all students are involved. Including all employees in religious facilities security operations, and properly training them in observation, increases the number of eyes on the floor and improves the chances of detecting a threat.

Based on data collected as part of the U.S. Department of Homeland Security's Enhanced Critical Infrastructure Protection program on protective measures employed by Commercial Facilities, actions taken by religious facilities to address vulnerabilities to both intentional acts, e.g., attacks or sabotage, and natural disasters have been concentrated primarily in the areas of security management, physical security, and dependencies. The most widely adopted security management protective measures include suspicious package procedures, managing information sharing, and security communication. Regarding physical security, attention has been focused on the development of illumination, building envelope, and closed circuit television. Effort also has been expended on reducing dependencies on critical products, transportation, and information technology.

Table 2 identifies baseline protective measures, some of which have been adopted by various religious facilities, which can be used to address the vulnerabilities summarized in Section 3.1.[4]

Table 2: Potential Baseline Protective Measures

	Vulnerability			
	Open Access	Gathering of People of a Particular Faith	Limited Security Budget	Natural Hazards
EQUIPMENT				
Perimeter barriers. Evaluate the need for perimeter barriers (e.g., fences, berms, concrete walls) around the facility.	✓	✓		
Facility perimeter. Define the facility perimeter and areas within the facility that require access control.	✓	✓	✓	
Doors and windows. Install barriers, e.g., blast film, to protect doors and windows from small arms fire and explosive blast effects.	✓	✓		
Visual surveillance. Provide visual surveillance capability for sensitive and critical assets at the facility**.**	✓	✓		
HVAC systems. Install barriers at HVAC systems to prevent the introduction of chemical, biological, or radiological agents into the building	✓	✓		
Clear zone. Establish a clear zone adjacent to sensitive or critical buildings; keep zone free of vegetation and other obstructions to	✓	✓	✓	

[4] The implementation of a protective measure at any time involves the commitment of resources in the form of people, equipment, materials, time, and money. Facility owners, local law enforcement, emergency responders, and State and local government agencies need to coordinate and cooperate in determining what measures should be implemented, how extensive they should be, and how long they should be kept in force in order to maximize security while staying within the bounds of available resources.

allow for continuous monitoring.				
Access restrictions. 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.	✓	✓		
Utility services. Ensure that the facility has adequate utility service capacity to meet normal and emergency needs	✓	✓	✓	✓
Communication. Install system(s) that provide communication with all individuals at the facility, including employees, congregation members, visitors, and emergency response teams.	✓	✓		✓
PERSONNEL				
Security Director. Designate an employee as Security Director.	✓	✓	✓	
Security force. Maintain an adequate security force using both employees and congregation volunteers.	✓	✓	✓	
Background checks. Conduct background checks on all employees.	✓	✓		
Security awareness training. Incorporate security awareness and appropriate response procedures for security situations into employee training programs.	✓	✓	✓	✓
Emergency response personnel. Ensure that an adequate number of emergency response personnel are on call at all times.	✓	✓	✓	✓
Emergency shutdown. Ensure that employees are familiar with procedures for shutting off utility services (e.g., electricity, natural gas) in emergency situations.	✓	✓	✓	✓
"See Something, Say Something." Encourage employees and the public to report anything that appears to be odd or suspicious.	✓	✓	✓	
PROCEDURES				
Monitoring and surveillance program. Evaluate needs and design a monitoring, surveillance, and inspection program that is consistent with facility operations and security requirements.	✓	✓	✓	
Security and emergency response planning. Develop a comprehensive security plan and emergency response plan for the facility.	✓	✓	✓	✓
Emergency response exercises. Conduct regular exercises with facility employees to test the security and emergency response plans.	✓	✓	✓	✓
Access by members and visitors. Limit access by congregation members and visitors to various areas in the facility to a level consistent with facility operations.	✓	✓	✓	
Vehicle restrictions. Keep vehicles away from critical assets and from areas where large numbers of people congregate.	✓	✓	✓	
Illegally parked vehicles. Require that all illegally parked vehicles be moved or have them towed.	✓	✓	✓	
Suspicious packages. Train personnel responsible for receiving deliveries to recognize suspicious mail, packages, and shipments.	✓	✓	✓	
Status of equipment. Check the status of all emergency response equipment and supplies on a regular basis.	✓	✓	✓	✓
Evacuation. Identify entry and exit points to be used in emergencies.	✓	✓	✓	✓
Monitor visitors. Continuously monitor all people entering and leaving the facility; train monitors to detect suspicious behavior.	✓	✓		
Trash containers. Secure dumpsters and other trash containers to prevent the hiding of explosives or other hazardous materials	✓	✓	✓	

Notification. Develop a notification protocol that specifies who should be contacted in emergencies.	✓	✓	✓	✓
INFORMATION SHARING				
Communication with law enforcement. Establish liaison and regular communication with local law enforcement and emergency responders.	✓	✓		✓
CYBER SECURITY				
Security plan for computer and information systems. Develop and implement a security plan for computer and information systems hardware and software, including a recovery and restoration plan to return computer systems to full functionality after an incident.	✓	✓		
Protect sensitive information. Require employees to use a specific login and unique password to access their electronic files.	✓	✓	✓	
Information control. Eliminate information from facility Web site that might aid potential adversaries in planning an attack.	✓	✓	✓	

Table 3 identifies additional protective measures religious facilities should consider in the case of a heightened alert.

Table 3: Potential Heightened Alert/Threat Protective Measures

	Vulnerability			
	Open Access	Gathering of People of a Particular Faith	Limited Security Budget	Natural Hazards
EQUIPMENT				
Portable pedestrian/vehicle barriers. Install lightweight barriers that are easy to store but can be quickly deployed against VBIEDs and IEDs.	✓	✓		
PERSONNEL				
Key staff. Assign key staff additional duties during and after an incident.	✓		✓	✓
PROCEDURES				
Continuous monitoring. Continuously monitor all vehicles approaching the facility for signs of threatening behavior. Continuously monitor all people entering and leaving the facility for suspicious behavior.	✓	✓		
Evacuation. During a major incident, have a plan to evacuate employees, congregants, and visitors out of the building.	✓	✓		✓
INFORMATION SHARING				
Fusion centers. Join a local/state fusion center to share intelligence about potential threats or to alert facility about an imminent attack.	✓	✓	✓	✓

References

DOJ, 2010, "Hate Crime Statistics 2009," [http://www2.fbi.gov/ucr/hc2009/victims.html], Website visited on March 4, 2013.

DHS, 2007, "Dams Sector Security Awareness Guide: A Guide for Owners and Operators."

FEMA, 2012, "Primer to Design Safe School Projects in Case of Terrorist Attacks and School Shootings," Buildings and Infrastructure Protection Series, FEMA-428/BIPS-07/January 2012, Edition 2.

FEMA, 2005, "A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings," Risk Management Series, Risk Assessment, FEMA 452 / January 2005.

FEMA, 2009, "Are You Ready? An In-Depth Guide to Citizen Preparedness," June 4 [http://www.fema.gov/areyouready/index.shtm].

FEMA, 2011, "Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings," Buildings and Infrastructure Protection Series, FEMA-426/BIPS-06/October 2011, Edition 2.

Grammich, C., K. Hadaway, R. Houseal, D. Jones, A. Krindatch, R. Stanley, and R. Taylor. 2012, *2010 U.S. Religion Census: Religious Congregations & Membership Study.* Association of Statisticians of American Religious.

Maryland, [http://www.mcac.maryland.gov/how_to_help/TerrorismIndicators.html]

NJOHSP, n.d., "Terrorism Indicators: Eight Signs of Terrorism," [http://www.njhomelandsecurity.gov/press-room/publications.html].