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

Infrastructure Protection Report Series

Common Vulnerabilities, Potential Indicators, and Protective Measures: Houses of Worship

October 2015

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. Christian (e.g., Protestant, Catholic, Orthodox Christian, and Latter-day Saints) assemblies account for nearly 97 percent of U.S. congregations.[1] The average congregation has a median attendance of 60 people at its main worship service.[2] Religious facilities often host regular worship services, and some facilities include schools, childcare centers, administrative offices, residences, and other resources for members of the community. Some religious facilities, such as the Washington National Cathedral, are national icons.

Potential threats to religious facilities can originate from disaffected individuals (e.g., employees or outsiders) and from domestic and international terrorist groups. According to U.S. Department of Justice (DOJ) statistics, the approximately 17 percent of all hate crimes recorded in 2013 were directed at individuals because of a bias against a religious belief.[3] The DOJ statistics indicate that nearly three-fourths of hate crimes motivated by religious bias targeted non-Christian victims: most were directed against Jews. Racial bias, the most prominent motivator of hate crime,[4] also may incite threats against religious facilities as the majority of congregations in the United States involve members who are of the same race.[5]

Deliberate Attacks

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 on religious facilities can involve a variety of different methods, including active shooters; improvised explosive devices (IEDs); vehicle-borne IEDs (VBIEDs); and/or arson. As the following examples demonstrate, deliberate attacks on religious facilities are a real threat that can inflict considerable harm.

- In June 2015, a man attended a Bible study at Emanuel African Methodist Episcopal Church in Charleston, South Carolina, for approximately 1 hour before shooting and killing nine people.[6]
- In February 2015, a man allegedly burned down one of three buildings at the Quba Islamic Institute in Houston.[7]

[1] 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.

[2] National Congregations Study, 2012, "Summary Tables," http://www.soc.duke.edu/natcong/Docs/SummaryTables.pdf, accessed July 13, 2015.

[3] U.S. Department of Justice, 2014, "Hate Crime Statistics, 2013," Federal Bureau of Investigations, https://www.fbi.gov/about-us/cjis/ucr/hate-crime/2013/topic-pages/incidents-and-offenses/incidentsandoffenses_final, accessed July 14, 2015.

[4] Ibid

[5] National Congregations Study, 2012, "Summary Tables," http://www.soc.duke.edu/natcong/Docs/SummaryTables.pdf, accessed July 13, 2015.

[6] Knapp, A., 2015, "Church Shooting Suspect Dylann Roof Returned to a City in Mourning," The Post and Courier, June 18, http://www.postandcourier.com/article/20150618/PC16/150619404, accessed July 2, 2015.

- In October 2012, a gunman entered the World Changers Church International in suburban Atlanta and shot and killed a volunteer who was leading a prayer group.[8]
- In August 2012, a gunman shot and killed six people and wounded three others at a Sikh Temple in Oak Creek, Wisconsin. The gunman then shot and critically wounded a responding police officer before shooting and killing himself.[9]

Individuals, small teams of a few perpetrators, or larger groups acting in a coordinated fashion can carry out attacks. The threats of greatest concern to religious facilities include:

Active Shooter and Small Arms Attack - Adversaries can launch these attacks using conventional firearms, automatic weapons, explosives, or similar weapons to harm people indiscriminately or take hostages.

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. Attackers can carry an IED into a religious facility via an individual (e.g., a suicide bomber) or can deposit it in an unnoticed location for detonation at a later time using a timer or remote control.

Vehicle-Borne Improvised Explosive Device - Religious facilities are also vulnerable to VBIED attacks—IEDs loaded into a vehicle (car, truck, or motorcycle). Adversaries can park the vehicle close to a religious facility and near areas where large numbers of people gather, or they can crash the vehicle through barriers and detonate the explosives. VBIEDs are much larger and more dangerous than IEDs carried by an individual.

Arson - Arsonists can set intentional fires 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.

Sabotage, Vandalism, and Theft - Sabotage, vandalism, and theft of religious artifacts are also concerns for religious facilities. Sabotage of equipment, such as of the heating, ventilation, and air-conditioning (HVAC) system, could disrupt religious ceremonies and other activities that take place at a religious facility. Acts of vandalism, such as those involving the defacement or destruction of religious symbols, and the theft of religious artifacts, may have psychological and emotional effects on congregations. In addition, they may incur costly repairs for organizations with limited resources.

Chemical, Biological, or Radiological Attack - Attackers can use chemicals as weapons, including toxic industrial chemicals (e.g., ammonia, hydrogen fluoride, and chlorine) and chemical warfare agents (e.g., sarin, VX). They can bring these substances near or into a religious facility and disperse them using explosives. Although chemical warfare agents are not readily available, terrorists have procured and used them previously. Adversaries can introduce biological pathogens (e.g., anthrax, plague) into a facility through its HVAC system or spread them through direct contact (e.g., through contaminated letters delivered by mail). They can use radiological dispersal devices such as "dirty bombs" which use a conventional explosion to scatter radioactive materials. Radioactive materials are widely used in

[7] Horansky, A., 2015, "Islamic Mosque Burned in an Arson Fire Makes Major Motion to Forgive," KHOU.com, February 20, http://www.khou.com/story/news/local/2015/02/20/islamic-mosque-burned-in-an-arson-fire-makes-major-motion-to-forgive/23769913/, accessed June 1, 2015.

[8] CNN.com, 2012, "Authorities Arrest Man Suspected of Killing 1 at Georgia Megachurch," October 24, http://www.cnn.com/2012/10/24/justice/georgia-church-shooting, accessed July 28, 2015.

[9] FoxNews.com, 2012, "Gunman in Sikh temple shooting identified as ex-Army soldier Wade Michael Page," August 6, http://www.foxnews.com/us/2012/08/06/authorities-search-for-motive-in-deadly-shooting-at-wisconsin-sikh-temple/, accessed March 1, 2013.

laboratories, medical centers, food irradiation plants, and industrial facilities; adversaries may steal or otherwise acquire these materials from these locations.

Natural Hazards/Accidents

Natural hazards—including infectious diseases and illnesses, fire, and seismic and weather-related events (e.g., hurricanes, tornadoes, flash floods)—can also adversely impact religious facilities. Such hazards can affect the safety of religious facilities' employees and members, as well as the facility's ability to carry out normal operations.

- In April 2014, an EF-3 tornado, part of a storm system impacting 10 States, leveled Grace Falls Church in Fayetteville, Tennessee, and destroyed the pastor's home next to the church building.[10]
- In October 2012, Superstorm Sandy damaged or destroyed dozens of places of worship, including St. Elizabeth's Chapel-by-the-Sea in Ortley Beach, New Jersey, which was completely washed away.[11]

Wooden Church after Tornado Damage (Source: stock photo)

Potential Indicators of an Attack[12]

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 typically fall into the following categories: imminent attack indicators and surveillance indicators.

Imminent Attack Indicators - These indicators may show that an attack is imminent and that immediate action is required. Indicators of an imminent attack include people, vehicles, or packages that demonstrate unusual or suspicious behavior that requires an immediate response. Table 1 lists potential indicators of an imminent attack.

Surveillance Indicators - Surveillance indicators may provide evidence that religious facilities are under surveillance by individuals planning an attack. One indicator of potential surveillance includes persons in the vicinity of religious facilities intending to gather information about the facility or its operations and protective measures. Table 1 outlines potential indicators that religious facilities may be under surveillance.

[10] Elk Valley Times, 2015, "Church Rebuilds One Year after Devastating Tornado," May 13, http://www.elkvalleytimes.com/church-rebuilds-one-year-after-devastating-tornado/, accessed July 14, 2015.

[11] Otterman, S., 2012, "For Congregation Leaders, Hurricane Is Taking a Toll," New York Times, November 12, http://www.nytimes.com/2012/11/13/nyregion/regional-places-of-worship-seek-to-rebuild.html?adxnnl=1&smid=pl-share&adxnnlx=1362157308-vmxZINbz0XRn+BhhI4ujZQ, accessed March 1, 2013.

[12] Indicators identified in this section draw from information found in U.S. Department of Homeland Security (DHS) (2007) and New Jersey Office of Homeland Security & Preparedness (NJOHSP) (undated), as well as information gathered during 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 inquiring excessively about practices pertaining to the facility and its operations or the facility's supporting infrastructure (e.g., telecommunications, electricity, 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 (ID) 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.

Religious facilities should establish communication channels with local law enforcement to maintain awareness of potentially threatening situations in the area and to piece together information from their facility with information from the surrounding area.

Common Vulnerabilities[13]

A variety of factors—such as 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 "soft targets"—contribute to challenges facing religious facilities in terms of protection and security. Violent attacks at religious facilities have highlighted vulnerabilities and have offered valuable lessons for protecting the facilities, the people who attend them, and the employees who work in them. In addition, religious facilities often become disaster relief centers following natural disasters and other mass-casualty events. Effective planning and preparedness training for such incidents enables religious facilities personnel to identify their potential roles in relief efforts.

This section identifies key common vulnerabilities associated with religious facilities and security and resilience measures that facility personnel can adopt to address those vulnerabilities. Although these potential vulnerabilities do not all apply to all religious facilities, they have been identified as priority focus areas for religious facilities management and security personnel to review. This section is informed

[13] Material in this section is based, in large part, on Federal Emergency Management Agency (FEMA) (2005, 2011, 2012), Federal Bureau of Investigation (FBI)/DHS (2012), and DHS (undated and 2013).

by data collected by U.S. Department of Homeland Security Protective Security Advisors since 2009 on vulnerabilities and security resilience measures at religious facilities across the United States, who voluntarily participated in security surveys.

Open Access

- **Unrestricted access to religious services.** In general, religious facilities are open to all, at least during 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 a potential adversary's access to the facility.
- **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. At all but one of the religious facilities surveyed, uncontrolled parking areas permit vehicles to park within 400 feet of the facility.
- **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 proximity can make maintaining effective perimeter security more difficult, cost-prohibitive, and counter to the facility's overall goals of community engagement.

The Islamic Center, Washington, DC (Source: stock photo)

- **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 features include parking areas, driveways on facility grounds, and nearby streets. Usually no vehicle barriers exist near the main entrances or other vulnerable parts of the buildings. About two-thirds of facilities surveyed have a high-speed avenue of approach; most do not use barriers to mitigate this vulnerability or to enforce standoff distance from the facility.
- **Lack of control of vendor and contractor personnel.** Individuals who deliver parcels or are hired to perform construction or repair work often receive unescorted access to religious facilities without inspection of the packages they deliver or materials they bring into the facility. About half of the religious facilities surveyed do not have procedures to address suspicious packages.
- **Unprotected utilities.** Religious facilities generally leave HVAC units and other critical building utility supply components (e.g., water, electric power, and natural gas service) easily accessible.

Gathering of People of a Particular Faith - A religious facility attracts a group of people of like faith at a single location at specified times. This gathering makes the facility a ready target for an adversary seeking to attack that particular group of people. Easy identification of the specific faith, either by facility configuration or signage, increases this vulnerability. Some religious facilities have a larger average weekly attendance of 2,000 or more. The largest of these "megachurches" in the United States are typically Protestant and have between 15,000 and 45,000 members.[14] Megachurches may have security personnel, usually volunteers or off-duty police officers, to direct traffic and provide security for the large numbers of people gathered onsite.

Limited Security Budget - Many religious facilities have small budgets that the facility uses primarily to pay for basic operations and to provide services to the congregation and surrounding communities. Many do not have the financial resources to implement security measures. As a result, religious facilities may not employ a security manager or have a written security plan.

Protective Measures

Security and resilience measures include equipment, personnel, and procedures designed to protect a facility against threats and hazards and to mitigate the effects of an adverse event. Some measures are permanent features that provide routine protection for a facility. Others are implemented or intensified only during times of heightened alert.

The relatively open access to religious facilities' building(s) and grounds makes it difficult to secure them. Security measures should be comprehensive, integrating equipment, personnel, procedures, and information sharing to ensure involvement of all employees and volunteers. Including all employees in security operations at religious facilities, and training them in observation skills, increases the number of eyes "on the floor" and improves the chances of detecting a threat.

Based on security survey data, religious facilities typically have a relatively low security and resilience posture. Actions that religious facilities have taken to address vulnerabilities to both intentional acts (e.g., attacks or sabotage), and natural disasters center primarily in the areas of security management, recovery mechanisms, and physical security. The most widely adopted security management protective measures include sensitive information management, suspicious-package procedures, and security information communication. With recovery mechanisms, religious facilities have focused attention on reducing the time necessary for the facility to recover full operations after losing significant components and critical resources. For physical security, activities have centered on security measures related to illumination, building envelope, and parking.

The table below identifies security and resilience measures that may be appropriate for religious facilities. Some protective measures identified below may not be feasible for individual facilities (particularly smaller facilities with limited budgets and staff) due to resource constraints. In addition, religious facilities may perceive select measures identified in this table as conflicting with their commitment to open access. However, these protective measures provide a starting point for discussion among stakeholders at religious facilities—including leadership, security and emergency response personnel, and congregants—on decisions and tradeoffs involved in safeguarding their facilities from natural and manmade hazards.

[14] Scribner, H., 2014, "15 Biggest Megachurches in America," Deseret News, August 14, http://national.deseretnews.com/article/2049/15-biggest-megachurches-in-america.html, accessed July 20, 2015.

Table 2: Potential Baseline Protective Measures

Protective Measures	Vulnerable Operating Conditions			
	Open Access	Mass Gathering	Limited Security Budget	Natural Hazards
EQUIPMENT				
Facility perimeter. Define the facility perimeter and areas within the facility that require access control.	✓	✓		
Perimeter barriers. Evaluate the need for perimeter barriers (e.g., fences, berms, concrete walls) around the facility to demarcate the boundary of the site to protect against trespassing; to provide access control by channeling individuals through authorized access points; and/or to protect against unauthorized entry by providing increased access delay and more time for assessment.	✓	✓		
Mitigate high-speed avenues of approach. Evaluate vehicle traffic patterns near the facility. Design and implement strategies to reduce vehicle speeds, improve pedestrian safety, and reduce the threat of vehicle approach velocities.	✓	✓		
Enforce standoff. Install barriers to increase standoff distance and reduce damage from a potential explosive device. Options include, but are not limited to, fixed and retractable bollards, engineered planters, heavy objects, trees, walls, landscape barriers, water obstacles, and Jersey barriers.	✓	✓		
Environmental design. Employ Crime Prevention Through Environmental Design principles, concepts, and strategies (e.g., water barriers, landscaping, high curbs, shallow ditches) to provide enhanced penetration delay. Consult Appendix A of *Site and Urban Design for Security: Guidance against Potential Terrorist Attacks (FEMA 430)* and Tables 2.4 and 2.5 of *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS 06)* for more information.	✓	✓		
Closed-circuit television (CCTV). Explore the feasibility of installing a comprehensive CCTV system onsite. Evaluate the need for real-time monitoring of the CCTV system based on the security requirements of the facility	✓	✓		
Illumination maintenance program. Establish a maintenance protocol to ensure that illumination system components are regularly inspected and repaired or replaced as necessary. Ensure that lighting fixtures are clean and properly aimed.	✓	✓		
Secure utility equipment. Secure components of critical utility systems inside and outside the facility against unauthorized access.	✓	✓		
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.	✓	✓		
Doors and windows. Install secure locks on all external and internal doors and windows with quick-release capability from within for emergency escape.	✓	✓		
Backup power. Evaluate power requirements for the facility to maintain core operations, and install backup power equipment accordingly. At a minimum, ensure all life-safety services have backup power.	✓	✓		✓

Table 2: Potential Baseline Protective Measures

Protective Measures	Vulnerable Operating Conditions			
	Open Access	Mass Gathering	Limited Security Budget	Natural Hazards
Communication. Install system(s) that provide for communication with all individuals at the facility, including employees, congregation members, visitors, and emergency response teams.	✓	✓		✓
Emergency response equipment. Ensure the facility necessary equipment to respond to a crisis. For example, ensure that emergency communications equipment is present and operable. Provide a secondary means of communications as a backup. Consider whether master keys are readily available to provide to first responders so that they have complete access to the facility in an emergency. Maintain a cache of first aid supplies and disperse them throughout the facility.	✓	✓		✓
PERSONNEL				
Security manager. Designate a security manager and task that person with developing, implementing, and coordinating all security-related activities.	✓	✓	✓	
Emergency manager. Designate an emergency manager to develop, implement, and coordinate all emergency management-related activities.	✓	✓	✓	✓
Background checks. Explore feasibility of conducting comprehensive background checks on facility personnel.	✓	✓		
Security awareness training. Incorporate security awareness and appropriate response procedures for security situations into employee and volunteer training programs.	✓	✓	✓	
If You See Something, Say Something™. Raise awareness among the congregation of potential threats and vulnerabilities. Encourage facility personnel and members of the congregation to report anything that appears to be odd or suspicious.	✓	✓	✓	
Emergency response training. Incorporate emergency response into employee and volunteer training programs. Ensure personnel are aware of their roles and responsibilities during a crisis.	✓	✓	✓	✓
PROCEDURES				
Monitoring and surveillance program. Evaluate the facility's security requirements and design a monitoring, surveillance, and inspection program that is consistent with facility operations and security requirements. Provide visual surveillance, and train system monitors to detect suspicious behavior.	✓	✓		
Security planning. Review, update, and validate the security plan regularly. Develop a comprehensive security plan specific to the facility if one does not already exist. The plan should address issues such as the following: protection of building occupants; protection of sensitive information; protection of funds; facility access control procedures; suspicious activity reporting procedures; employee termination procedures; parking security; background checks; prohibited items; security force; end-of-day security checks; control and accountability of equipment (including keys); electronic security systems (including CCTV); physical security inspection programs; and security awareness training programs. Train personnel on the plan, and exercise the plan at least once a year.	✓	✓	✓	

Table 2: Potential Baseline Protective Measures

Protective Measures	Vulnerable Operating Conditions			
	Open Access	Mass Gathering	Limited Security Budget	Natural Hazards
Threat levels. Incorporate a threat level system into the security plan.	✓	✓	✓	
Security information reporting. Develop a plan and procedures for reporting threats, threatening behavior, and concerning behavior that occur or are observed at the facility, and make the congregation aware of the plan.	✓	✓	✓	
Access by members and visitors. Consider limiting access by congregation members and visitors to select areas in the facility (e.g., offices, storage areas, utility rooms).	✓	✓	✓	
Accountability for children. Establish an accountability system for children attending classes, events, etc., such as a secure child check-in/check-out system.	✓	✓	✓	✓
Vehicle restrictions. Explore the feasibility of prohibiting parking near critical utility equipment.	✓	✓	✓	
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.	✓	✓	✓	
Trash containers. Secure dumpsters and other trash containers to prevent the hiding of explosives or other hazardous materials.	✓	✓	✓	
Emergency response planning. Review, update, and validate the emergency plan regularly. Develop a comprehensive emergency plan specific to the facility if one does not already exist. Train personnel on the plan, and exercise the plan at least once a year. Refer to the Guide for Developing High-Quality Emergency Operations Plans for Houses of Worship released by the White House in 2013 for more information. A recorded webinar that includes presentations on the Guide, a brief question and answer session, and information on how to access more information and resources is available through the Readiness and Emergency Management for Schools Technical Assistance Center Website and on YouTube. Train personnel on the plan, and exercise the plan at least once a year.	✓	✓	✓	✓
Evacuation, lockdown, and shelter-in-place. Review plans and procedures for evacuation, lockdown, and shelter-in-place.	✓	✓	✓	✓
Consideration of access and functional needs. Ensure emergency plans provide for the needs of people with disabilities and other access and functional needs, particularly when considering evacuation procedures and staging areas.	✓	✓	✓	✓
Safe areas. Establish safe areas within the facility for assembly and refuge during crises.	✓	✓	✓	✓
Status of equipment. Check the status of emergency response equipment and supplies on a regular basis.	✓	✓	✓	✓
Emergency shutdown. Ensure that the appropriate personnel are familiar with procedures for shutting off utility services (e.g., electricity, natural gas) in emergency situations.	✓	✓	✓	✓
Emergency communications. Establish and implement an emergency communications system such as phone trees or mass text messaging.	✓	✓		✓

Table 2: Potential Baseline Protective Measures

Protective Measures	Vulnerable Operating Conditions			
	Open Access	Mass Gathering	Limited Security Budget	Natural Hazards
Incident management. Establish an incident management and command center dedicated to facilitating the coordination and support of emergency management activities.	✓	✓		✓
INFORMATION SHARING				
First responder interaction. Establish liaison and regular communication with local law enforcement, fire response agencies, and emergency medical services. Coordinate security and emergency plans with first responders to enhance incident response. Conduct onsite visits with first responders to increase their familiarity with the facility.	✓	✓	✓	✓
Security and emergency preparedness working groups. Join relevant security and emergency preparedness working groups. Establish liaisons and regular communications with Federal, State, and local-level groups, as well as private sector/industry groups, to share expertise and prepare to better respond to security incidents and emergencies.	✓	✓	✓	✓
State and local emergency operation centers (EOCs). Collaborate with a State and/or local EOC to facilitate the exchange of real-time situational awareness information.	✓	✓	✓	✓
Fusion centers. Join a State or local fusion center to share intelligence about potential threats or to alert facility about an imminent attack.	✓	✓	✓	✓
CYBERSECURITY				
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 Website that might aid potential adversaries in planning an attack.	✓	✓	✓	

References

CNN.com, 2012, "Authorities Arrest Man Suspected of Killing 1 at Georgia Megachurch," October 24, http://www.cnn.com/2012/10/24/justice/georgia-church-shooting, accessed July 28, 2015.

DHS, undated, "Common Vulnerability: Significant Numbers of People Gathered in a Single Location at Specified Times," TRIPwire Community Gateway.

DHS, 2007, *Dams Sector Security Awareness Guide: A Guide for Owners and Operators*.
DHS, 2013, *Houses of Worship Security Practices Guide*, May, http://www.illinois.gov/ready/plan/Documents/DHS_Houses_of_Worship_Security_Practices_Guide.pdf, accessed July 13, 2015.

U.S. Department of Justice, 2014, "Hate Crime Statistics, 2013," *Federal Bureau of Investigations*, https://www.fbi.gov/about-us/cjis/ucr/hate-crime/2013/topic-pages/incidents-and-offenses/incidentsandoffenses_final, accessed July 14, 2015.

Elk Valley Times, 2015, "Church Rebuilds One Year after Devastating Tornado," May 13, http://www.elkvalleytimes.com/church-rebuilds-one-year-after-devastating-tornado/, accessed July 14, 2015.

FBI/DHS Joint Intelligence Bulletin, 2012, "Recent Active Shooter Incidents Highlight Need for Continued Vigilance," December 27, Unclassified/For Official Use Only.

FEMA, 2014, *Are You Ready? An In-Depth Guide to Citizen Preparedness*, August, http://www.fema.gov/media-library-data/20130726-1549-20490-4633/areyouready_full.pdf, accessed June 3, 2015.

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, http://www.dhs.gov/xlibrary/assets/st/bips07_428_schools.pdf, accessed July 28, 2015.

FEMA, 2011, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, Buildings and Infrastructure Protection Series, FEMA-426/BIPS-06/October 2011, Edition 2, http://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, accessed July 28, 2015.

FEMA, 2005, "A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings," Risk Management Series, Risk Assessment, FEMA 452 / January 2005, http://www.fema.gov/media-library-data/20130726-1524-20490-7395/fema452_01_05.pdf, accessed July 28, 2015.

FoxNews.com, 2012, "Gunman in Sikh temple shooting identified as ex-Army soldier Wade Michael Page," August 6, http://www.foxnews.com/us/2012/08/06/authorities-search-for-motive-in-deadly-shooting-at-wisconsin-sikh-temple/, accessed March 1, 2013.

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.

Horansky, A., 2015, "Islamic Mosque Burned in an Arson Fire Makes Major Motion to Forgive," *KHOU.com*, February 20, http://www.khou.com/story/news/local/2015/02/20/islamic-mosque-burned-in-an-arson-fire-makes-major-motion-to-forgive/23769913/, accessed June 1, 2015.

Knapp, A., 2015, "Church Shooting Suspect Dylann Roof Returned to a City in Mourning," *The Post and Courier*, June 18, http://www.postandcourier.com/article/20150618/PC16/150619404, accessed July 2, 2015.

National Congregations Study, 2012, "Summary Tables," http://www.soc.duke.edu/natcong/Docs/SummaryTables.pdf, accessed July 13, 2015.

NJOHSP, undated, "Terrorism Indicators: Eight Signs of Terrorism" http://www.jcrcny.org/wp-content/uploads/2014/04/Religious-Facilities-IPRS-Report_APR-2014.pdf, accessed July 28, 2015.

Otterman, S., 2012, “For Congregation Leaders, Hurricane Is Taking a Toll,” *New York Times*, November 12, http://www.nytimes.com/2012/11/13/nyregion/regional-places-of-worship-seek-to-rebuild.html?adxnnl=1&smid=pl-share&adxnnlx=1362157308-vmxZINbz0XRn+BhhI4ujZQ, accessed March 1, 2013.

Sanders, Sam, 2015, “Investigators Probe Fires At 6 Black Churches In 5 Southern States,” National Public Radio, http://www.npr.org/2015/06/29/418490411/arsonists-hit-6-black-churches-in-5-southern-states, accessed September 23, 2015.

Scribner, H., 2014, “15 Biggest Megachurches in America,” *Deseret* News, August 14, http://national.deseretnews.com/article/2049/15-biggest-megachurches-in-america.html, accessed July 20, 2015.