Colorado Homeland Security Resources

for the

Faith Based Community

Table of Contents

Partnership Resources

U.S. Department of Homeland Security (DHS): Links to information on DHS missions to include preventing terrorism and enhancing security; managing our borders; administering immigration laws; securing cyberspace; and ensuring disaster resilience – includes the Daily Open-Source Information Report and travel security information. http://www.dhs.gov . The link to the DHS Critical Infrastructure Protection page, including many of the Infrastructure Protection Programs, is http://www.dhs.gov/files/programs/critical.shtm

The Counterterrorism Education Learning Lab (CELL): The CELL is a non-profit and non-partisan institution dedicated to educating citizens about one of the most important issues of our time - terrorism. The CELL's mission is to empower individuals and organizations with the tools to become more informed, prepared, and involved within their own communities in order to help combat the threat of terrorism. Their exhibit, Anyone – Anytime – Anywhere: Understanding the Threat of Terrorism, is a dynamic, interactive experience with content developed by world-renowned experts, that provides visitors with an in-depth of the history of terrorism, the methods terrorists employ, and the extent to which terrorism impacts societies around the world. http://www.thecell.org/

Colorado Emergency Preparedness Partnership (CEPP): The mission of the partnership is to strengthen the region's collective capacity to prevent, respond to, and recover from natural and human-caused disasters through effective public-private collaboration. http://www.thecepp.org/

Planning & Resilience Resources

Developing High Quality Emergency Operation Plans for Houses of Worship: The guide provided recommendations in the development of plans not only to respond to an emergency, but also outline how organizations can plan for preventing, protecting against, mitigating the impact of and recovering from these emergencies. The guide translates lessons learned from the Administration's work on national preparedness to the school, IHE, and house of worship contexts, ensuring that these critical assets are benefitting from recent advancements in the emergency planning field. The guide introduces houses of worship to a new approach to planning, that includes walking through different emergency scenarios to create a course of action for each objective the team is trying to accomplish. The guide emphasizes that successful planning requires all stakeholders be engaged in the planning process from the start – including community partners such as local law enforcement, fire officials, EMS and emergency management staff. https://www.fema.gov/media-library/assets/documents/33007

Nonprofit Security Grant Program: The Nonprofit Security Grant Program provides funding support for hardening and other physical security enhancements to nonprofit organizations that are at high risk of terrorist attack and located within one of the specific Urban Area Security Initiative areas. The NSGP also serves to promote coordination and collaboration in emergency preparedness activities among public and private community representatives as well as state and local government agencies. https://www.fema.gov/nonprofit-security-grant-program

Standard Response Protocol: Courtesy of the "i love u guys" Foundation, the Standard Response Protocol (SRP) is based not on individual scenarios but on the response to any given situation. Like the Incident Command System (ICS), SRP demands a specific vocabulary but also allows for great flexibility. The premise is simple - there are four specific actions that can be performed during an incident. When communicating these, the action is labeled with a "Term of Art" and is then followed by a "Directive." Execution of the action is performed by active participants, including students, staff, teachers and first responders. http://www.iloveuguys.org/srp.html

How to Assess the Safety & Security of Your Place of Worship: This material was developed to: 1.) Give you the information, ideas and guidelines you need to conduct an effective assessment of your place of worship, as it relates to people, places, assets, processes and programs, as well as emergency planning and continuity planning; and 2.) Encourage a focused and balanced approach to safety and security planning.
http://www.santarosa.fl.gov/coad/documents/SafetyinChurch.pdf

Security Concerns for Churches: The Role of Greeters and Ushers: Greeters and ushers can have a leadership role in safety, security and emergency planning related to many concerns in a place of worship. Their knowledge and experiences about church schedules, members and visitors and concerns or problems they have observed or handled, can make them invaluable contributors to the overall church security program.
http://storage.cloversites.com/theriverconference/documents/The%20Greeter%20and%20Usher%20Role%20In%20Church%20Security.pdf

Colorado School Safety Resource Center (CSSRC): The mission of the Colorado School Safety Resource Center (CSSRC) is to collaboratively assist local schools and communities to create safe and positive school environments for Colorado students in all pre-K-12 and higher education schools. The CSSRC provides consultation, resources, training, and technical assistance to foster safe and secure learning environments, positive school climates, and early intervention to prevent crisis situations. The CSSRC supports schools and local agencies in their efforts to prevent, prepare for, respond to, and recover from all types of emergencies and crisis situations. www.Colorado.gov/CSSRC

Safe2Tell: Designed to help students anonymously report any threatening behavior that endangers them, their friends, family, or community. http://safe2tell.org/

Netsmartz **Worksop:** NetSmartz Workshop is an interactive, educational program of the National Center for Missing & Exploited Children® (NCMEC) that provides age-appropriate resources to help teach children how to be safer on- and offline. The program is designed for children ages 5-17, parents and guardians, educators, and law enforcement. With resources such as videos, games, activity cards, and presentations, NetSmartz entertains while it educates. Our Goals: Educate children on how to recognize potential Internet risks; Engage children and adults in a two-way conversation about on- and offline risks; and Empower children to help prevent themselves from being exploited and to report victimization to a trusted adult. http://www.netsmartz.org/Parents

Ready Colorado: READYColorado.com is designed to help every Coloradan become prepared to respond to and recover from a wide array of disasters ... both natural and human-caused. www.readycolorado.com

Business Continuity Planning Suite: This software was created for any business with the need to create, improve, or update its business continuity plan. The Suite is scalable for optimal use by organizations of any size and consists of a business continuity plan (BCP) training, automated BCP and disaster recovery plan (DRP) generators, and a self-directed exercise for testing an implemented BCP. Businesses can utilize this solution to maintain normal operations and provide resilience during a disruption. http://www.ready.gov/business-continuity-planning-suite

Community Emergency Response Teams: Welcome to the Community Emergency Response Team (CERT) webpage. Here you can find resources, training and information about the CERT Program. CERT educates individuals about disaster preparedness for hazards that may impact their area and trains them in basic disaster response skills, such as fire safety, light search and rescue, team organization, and disaster medical operations. Using training learned in the classroom and during exercises, CERT volunteers can assist others in their community following a disaster when professional responders are not immediately available to help. CERT volunteers are also encouraged to support emergency response agencies by taking an active role in emergency preparedness projects.
https://www.fema.gov/community-emergency-response-teams#

Assessment Resources

Infrastructure Survey Tool (IST): The IST is a facility assessment that focuses on identifying gaps and providing options for consideration to enhance overall resiliency. The IST uses analysis of critical assets and current security measures via the creation of a math based, updateable Protective Measures Index (PMI), to identify vulnerabilities and develop mitigation strategies. IST areas of focus include: facility overview and significance, barriers, building envelope, critical products, dependencies (natural gas, communications, electricity, IT, cyber, transportation, water, wastewater), entry control, illumination, information sharing, parking, physical security, protective measures, security force, security management, security systems, significant assets, and business continuity. As an outcome to this visit, you will receive a PMI Dashboard that graphically illustrates your facilities' current security posture as well as a written report that highlights our observations, noted vulnerabilities, your commendable actions, and prospective options for consideration.

Infrastructure Visualization Platform (IVP): The IVP is a tactical multimedia tool that creates an interactive visual guide of any location by integrating various types of data. The IVP generates a 360-degree geospherical video and geospatial panoramic imagery of facilities, surrounding areas, transportation routes, and other areas of interest to provide emergency response personnel and infrastructure owners/ operators with a cross-platform tool that allows them to present data, make quick and informed decisions, and confidently respond to an incident. The information resulting from a IVP assessment is provided via an interactive IVP Report which incorporates the collected photos and video as well as the user-supplied data, including evacuation plans, standard operating procedures, geospatial and aerial facility views, schematic/floor plans, and vulnerability assessments.

Online Training Resources

FEMA Emergency Management Institute (EMI): Through its courses and programs, EMI serves as the national focal point for the development and delivery of emergency management training to enhance the capabilities of federal, state, local, and tribal government officials, volunteer organizations, and the public and private sectors to minimize the impact of disasters on the American public. Click http://training.fema.gov/EMIWeb//IS/crslist.asp. This link takes you to a list of about 60 independent study courses. Examples include: IS-100: Introduction to the Incident Command System (ICS); IS-546: Continuity of Operations (COOP) Awareness Course; IS-700: National Incident Management System (NIMS); IS-800: National Response Framework (NRF); IS-860: National Infrastructure Protection Plan (NIPP)

8 Signs of Terrorism Video: Terrorist operations usually begin with extensive planning. You can help prevent and detect terrorism, and other types of crime, by watching out for suspicious activities and reporting them to the proper authorities. The video, narrated by John Elway, is a partnership between the CELL, CIAC, DHS, and FBI. Be alert for the eight signs of terrorism! http://www.youtube.com/watch?feature=player_embedded&v=iWnKvhVnl9U

Active Shooter, What Can You Do: The Department of Homeland Security (DHS) announces the availability of a new Independent Study Course titled: *Active Shooter, What You Can Do (IS-907),* a no-cost training course developed to provide the public with guidance on how to prepare for and respond to active shooter crisis situations. A certificate from FEMA EMI is awarded to participants who complete the course and pass a short final exam. This new online training is available through the Federal Emergency Management Agency (FEMA) Emergency Management Institute (EMI) at http://training.fema.gov/EMIWeb/IS/IS907.asp

Run. Hide. Fight. Surviving An Active Shooter Event Video: This video, produced by the Houston Mayor's Office of Public Safety and Homeland Security, dramatizes an active shooter incident in the workplace. Its purpose is to educate the public on how to respond during such an incident. Warning: The initial sequence in this video may be disturbing. https://www.fbi.gov/about-us/cirg/active-shooter-and-mass-casualty-incidents/run-hide-fight-video

Active Shooter Preparedness: The Department of Homeland Security (DHS) aims to enhance preparedness through a ”whole community” approach by providing training, products, and resources to a broad range of stakeholders on issues such as active shooter awareness, incident response, and workplace violence. In many cases, there is no pattern or method to the selection of victims by an active shooter, and these situations are by their very nature are unpredictable and evolve quickly. DHS offers free courses, materials, and workshops to better prepare you to deal with an active shooter situation and to raise awareness of behaviors that represent pre-incident indicators and characteristics of active shooters. http://www.dhs.gov/activeshooter

Onsite Training Resources

https://www.dhs.gov/bombing-prevention-training

Surveillance Detection Course for Law Enforcement & Security Professionals: This course, designed for municipal security officials, State and local law enforcement with jurisdictional authority over critical infrastructure facilities, and critical infrastructure operators and security staff of critical infrastructure facilities, provides participants with the skills and knowledge to establish surveillance detection operations to protect critical infrastructure during periods of elevated threat. Consisting of five lectures and two exercises, the course increases awareness of terrorist tactics, attack history, and illustrates the means and methods used to detect surveillance**.** (3-days, up to 25 participants)

IED Counterterrorism Workshop: This awareness level workshop is designed to enhance the knowledge of Law Enforcement and Private Sector security professionals by providing exposure to key elements of the improvised explosive device (IED) threat, surveillance detection methods and soft target awareness. The workshop illustrates baseline awareness and prevention actions that reduce vulnerabilities to counter the threat along with collaborating information sharing resources to improve preparedness. This designed approach better enables the owners and operators of critical infrastructure and key resources to deter, prevent, detect, protect against, and respond to terrorist use of explosives in the United States. (Four sessions over two days or two eight hour sessions over two days; up to 250 participants per session)

Protective Measures Course: This course is designed to provide executive and employee level personnel in the public/private sector with the knowledge to identify the appropriate protective measures for their unique sector. The course focuses on providing information pertaining to available protective measures and strategies for selecting which protective measures are most appropriate. The course focuses on teaching the student the threat analysis process, terrorist methodology and planning cycle, available protective measures, and determining which protective measures to employ. (Two days, up to 35 participants)

Bomb Making Materials Awareness Program: The Bomb Making Materials Awareness Program (BMAP) is a new and innovative program sponsored by the Department of Homeland Security (DHS) Office for Bombing Prevention (OBP). It is designed to increase private sector awareness of activities associated with bomb-making, including the manufacture of homemade explosives (HMEs). BMAP provides audience-appropriate awareness information on suspicious behavior, hazardous materials, precursor chemicals, and other bomb-making related information. It is communicated as part of DHS’s TRIPwire and National IED Prevention and Awareness Campaign and was developed in cooperation with the FBI.

Improvised Explosive Device (IED) Awareness/ Bomb Threat Management Workshop: Enhances participants’ knowledge, skills, and abilities concerning IEDs. Outlines specific safeties associated with bomb threat management and IED awareness, incidents, and prevention.

Improvised Explosive Device Search Procedures: Increases preparedness of security personnel and facility managers of sites that are hosting a special security event. Focuses on general safeties used for specialized search and explosives sweeps and can be tailored to meet specific participants’ needs.

Vehicle Borne IED Detection Course: This course improves participant's ability to successfully inspect for, detect, identify components of and respond to a Vehicle Borne Improvised Explosive Device (VBIED). The target audience consists of first responders, public safety officers, and private security professionals tasked with inspecting vehicles for contraband, explosives, or any dangerous goods. The course covers the VBIED threat, explosives, IEDs, and vehicle inspections, enabling participants to deter, protect against, and respond to terrorist use of explosives in the United States.

Suspicious Activity Reporting (SAR) Resources

The Nationwide SAR Initiative: The Nationwide Suspicious Activity Reporting (SAR) Initiative is a collaborative effort led by the U.S. Department of Justice (DOJ) in partnership with DHS, FBI, and State, local, tribal, and territorial law enforcement partners. This initiative provides law enforcement with another tool to help prevent terrorism and other related criminal activity by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information. Homeland Security is everyone's responsibility. If you wish to report suspicious information that you believe relates to terrorism, or that may result in the prevention of terrorism, please submit that information via the Colorado Information Analysis Center (CIAC) link found at http://dhsem.state.co.us/prevention-security/ciac. Your report will be immediately forwarded to the FBI, DHS, and local law enforcement. We always recommend contacting law enforcement as the first step.

Local Law Enforcement	**911**	(imminent activity)
Colorado Information Analysis Center (CIAC)	720-852-6705	(any suspicious activity)
TSA General Aviation Hotline	866-GA-SECURE	(suspicious general aviation activity)

If You See Something, Say Something: The nationwide "If You See Something, Say Something™" public awareness campaign - is a simple and effective program to raise public awareness of indicators of terrorism and terrorism-related crime, and to emphasize the importance of reporting suspicious activity to the proper local law enforcement authorities. The campaign was originally used by New York's Metropolitan Transportation Authority (MTA), which has licensed the use of the slogan to DHS for anti-terrorism and anti-terrorism crime related efforts. http://www.dhs.gov/if-you-see-something-say-something%E2%84%A2-campaign

Download an electronic copy of the "See Something, Say Something" campaign video. http://www.dhs.gov/xlibrary/videos/fema-tp.031011.zip. The video is 10-minutes in length. Click 'Save' to load this onto your hard drive (95MB zip file – becomes a .wmv file).

Community Awareness Program (CAP): The Community Awareness Program™ (CAP), hosted in partnership with the Counter-terrorism Education Learning Lab (The CELL) and the Colorado Information Analysis Center (CIAC), empowers citizens to help play a role in enhancing our community's safety. The CAP is a free, interactive course taught by members of the public safety community. It provides citizens with the basic tools needed to recognize and help prevent criminal activity and terrorism in the United States while preserving civil liberties protected by the U.S. Constitution. http://www.thecell.org/cap/

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

Infrastructure Protection Report Series

Potential Indicators, Common Vulnerabilities, 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 houses of worship, such as the Washington National Cathedral, are national icons.

Potential threats to houses of worship 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 further 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 houses of worship as the majority of congregations in the United States involve members who are of the same race.[5]

Potential 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 on houses of worship 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 houses of worship 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 houses of worship include:

Active Shooter and Small Arms Attack - Adversaries can launch these attacks using conventional firearms, automatic weapons, 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 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 – Houses of worship are also vulnerable to VBIED attacks—IEDs loaded into a vehicle (car, truck, or motorcycle). Adversaries can park the vehicle close to a 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 house of worship 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 houses of worship. 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

[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.

> 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 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 houses of worship. Such hazards can affect the safety of 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.
>
> **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 houses of worship intending to gather information about the facility or its operations and protective measures.

Potential indicators of an imminent attack, or that a facility may be under surveillance, are listed in Table 1.

[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 or weapons.
- 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.

Houses of worship should establish communication channels with local law enforcement to maintain awareness of potentially threatening situations in the area.

Common Vulnerabilities[13]

A variety of factors—such as the sheer number of houses of worship in the United States, the scheduling and predictability of times when members gather to worship (which facilitate surveillance and targeting), and the attractiveness of houses of worship as "soft targets"—contribute to challenges facing facilities in terms of protection and security. Violent attacks at houses of worship 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, houses of worship often become disaster relief centers following natural disasters and other mass-casualty events. Effective planning and preparedness training for such incidents enables houses of worship personnel to identify their potential roles in relief efforts.

[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).

This section identifies key common vulnerabilities associated with houses of worship and security and resilience measures that facility personnel can adopt to address those vulnerabilities. Although these potential vulnerabilities do not all apply to all houses of worship, they have been identified as priority focus areas for management and security personnel to review. This section is informed by data collected by U.S. Department of Homeland Security Protective Security Advisors since 2009 on vulnerabilities and security resilience measures at houses of worship across the United States, who voluntarily participated in security surveys.

1. Open Access

- **Unrestricted access to religious services.** In general, houses of worship 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, houses of worship may or may not be able to control a potential adversary's access to the facility.
- **Unrestricted access to peripheral areas.** Houses of worship 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 facilities surveyed, uncontrolled parking areas permit vehicles to park within 400 feet of the facility.
- **Proximity of houses of worship and neighboring facilities, especially in urban areas.** Many 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 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 without inspection of the packages they deliver or materials they bring into the facility.
- **Unprotected utilities.** Houses of worship generally leave HVAC units and other critical building utility supply components (e.g., water, electric power, and natural gas service) easily accessible.

2. **Gathering of People of a Particular Faith -** A house of worship 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 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.

3. **Limited Security Budget -** Many houses of worship 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, these 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 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, houses of worship typically have a relatively low security and resilience posture. Actions that houses of worship have taken to address vulnerabilities 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, houses of worship 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 measures related to illumination, building envelope, and parking.

The table below identifies security and resilience measures that may be appropriate for houses of worship. 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, 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 houses of worship—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.