Houses of Worship Security Practices Guide
May 2013

Table of Contents

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[1]. 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.

This guide will provide security practices for consideration by religious communities to deter threats, address hazards and risks, as well as minimize the damage from an incident in their religious facilities, including mass casualty events. The security practices discussed in this document offer a spectrum of options for consideration, from programmatic and procedural considerations to technological enhancements that religious facility officials/leadership may consider implementing based upon the most likely threats to their facilities and their available resources. The security practices guide includes options for consideration for developing a security plan that builds from existing comprehensive assessment efforts (e.g., culture and climate, institution threat assessment) and blends a number of security practices to achieve an effect where threats are either deterred, or delayed and detected in advance of creating harm. In the case of a detected threat, a security plan should provide for timely assessment of the threat, create time for selecting an appropriate response to a threat, and facilitate transition into an effective recovery if necessary. To be cost effective, the security plan should implement solutions that serve multiple safety or security objectives and ensure a safe environment.

The first step to developing a comprehensive religious facilities security program is to identify the threats that potentially jeopardize the physical well-being of the individuals in the religious facility. The next section will review some potential threats a religious facility may face.

2. Threats and Vulnerabilities

Identifying and evaluating a known or potential threat to a given facility is a preliminary component of a security assessment, the results of which will guide the process of developing a security plan. A proper plan will aim to deter a threat or mitigate a threat by reducing the religious facility's vulnerability to those threats. Potential threats to religious facilities can originate from disaffected individuals (e.g., employees, former members) or groups, outsiders, criminals, or domestic or 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 individuals because of a bias against a religious belief[2]. In addition to man-made threats, natural hazards can affect religious facilities directly (e.g., a tornado significantly damaging a place of worship), or indirectly, by adversely affecting upstream suppliers (e.g.,

---

[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] http://www2.fbi.gov/ucr/hc2009/victims.html

negative impact on electric utilities that, in turn, disrupts 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. As numerous events over the past several years have demonstrated, deliberate attacks on religious facilities are a real threat that can inflict considerable harm.

2.1   Threats

2.1.1   Natural Hazards/Accidents

Effective, comprehensive religious facility emergency management plans use an all-hazards approach to assess and address 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.

AP Photo Carolyn Kaster

- In October 2012, Superstorm Sandy damaged or destroyed dozens of places of worship. As one example, St. Elizabeth's Chapel-by-the-Sea was completely washed away[3].

2.1.2   Targeted Violence

In addition to threats posed by extreme acts of nature or man-made accidents, religious facilities are vulnerable to pre-planned attacks of targeted violence committed by individuals using a variety of tactics to inflict harm on a religious facility. Individuals who target a religious facility for harm could use firearms; improvised explosive devices (IEDs); vehicle-borne improvised explosive devices (VBIEDs); chemical, biological, or radiological attacks; or arson in order to inflict a number of casualties and damage to religious facilities. Perpetrators 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:

2.1.2.1   *Targeted Violence in Religious Facility Settings*

Individuals who target a religious facility for some act of violence could use conventional firearms, automatic weapons, explosives or similar weapons to harm individuals or take hostages. As numerous events over the past several years have demonstrated, deliberate attacks on religious facilities are a real threat that can inflict considerable harm.

---

[3] http://coastal.er.usgs.gov/hurricanes/sandy/

- 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[4].

2.1.2.2   Improvised Explosive Device (IED)

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.

2.1.2.3   Vehicle-Borne Improvised Explosive Device (VBIED)

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

2.1.2.4   Arson

Intentional fires can be set by using highly flammable materials (e.g., gasoline) tossed into a religious facility. Accelerants that promote the spread and intensity of a fire can be applied beforehand and then ignited. Arson is a threat both during and after normal hours of operation.

2.1.2.5   Chemical or Biological 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, ricin) 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).

2.1.2.6   Assassination and Kidnapping

Many terrorist acts have involved the assassination of key personnel or the kidnapping of individuals and hostage-taking. In addition, highly-visible religious figures or controversial religious figures may contribute to a higher risk environment.

---

[4] Sidhu, Dawinder S. "Lessons on Terrorism and 'Mistaken Identity' from Oak Creek, with a Coda on the Boston Marathon Bombings." *Colum. L. Rev. Sidebar* 113 (2013): 76-88.

2.2   Vulnerabilities

This section identifies key common vulnerabilities associated with religious facilities. 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. 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 sector-wide security- and protection-related challenges:

- **Prevention of attacks.** Since religious facilities generally provide an open atmosphere, facilities within their territories are vulnerable to deliberate malevolent acts by outside perpetrators. 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. In addition, the perception that religious facilities are "soft targets" and have little security may make them a more attractive target for individuals looking to carry out an attack on a large group of individuals.
- **Natural disaster/mass casualty events**. Religious facilities are generally exposed to various natural hazards (e.g., tornados, hurricanes, floods and earthquakes); as such, facilities are at a constant risk of being damaged. 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.

2.2.1   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, trained volunteers, 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 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.

2.2.2 Gatherings 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. Religious or customary garments, clothing or other items worn or displayed by persons of a particular faith may also increase identification of individuals belonging to a particular faith. In addition to religious services and special events, congregants often gather outside of religious facilities before and after religious services where little or no security or protection is afforded.

2.2.3 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, especially physical security equipment. Thus, for example, workers and volunteers may not undergo background checks.

2.2.4 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 and business continuity plans can provide the foundation for responding to unexpected or catastrophic events. When evaluating these types of plans, the 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 Prevention, Protection, and Mitigation

Prevention, protection, and mitigation address the steps that religious facilities and community partners can take to reduce or eliminate the risk to life and property. This section will highlight threat assessments, identify potential attack indicators, recommend possible protective measures for coordination with community partners, and discuss reporting procedures. An important element of an effective security program incorporates a process to achieve and maintain situational awareness and understanding about what is occurring in or around a religious facility. On a larger scale, it is important to maintain a general awareness of global and geopolitical events that could have potential security implications for communities and facilities here in the

U.S. Situational understanding and the ability to discover threats to the religious facility can be achieved and maintained by implementing a culture where leadership, staff, members, and visitors consciously evaluate available information from the institution environment to identify and assess potential threats of violence. Just as meteorologists rely on sensor data to accurately forecast the weather, religious facility personnel must rely on human and some technological sensors to collect and report religious facility environmental data to identify and assess potential threats. The sensors in a religious facility are not all technological; the majority of the best sensors are humans. In a religious facility setting, sensors can be the whole community surrounding the facility, facility staff, facility leadership, members, and visitors. A threat assessment team can be established to gather information and identify potential threats, as well as use that information to assess the nature of the threat, and select the most appropriate course of action to manage and mitigate that threat in order to maintain a safe environment.

Facility personnel can educate the religious community on how they can aid in the prevention of violence from threats. Facility personnel can socialize the religious community to recognize the behavioral indicators often associated with perpetrators of violence, communicate the importance of reporting their observations to police or religious facility leadership, develop processes to receive those reports and respond appropriately, conduct threat assessments to evaluate the threat report, and ensure that steps are taken to effectively interdict and mitigate a potential threat.

An individual not directly affiliated with the institution who may be planning to carry out some act of violence may come to the attention of law enforcement. Therefore, discovering external threats to a religious community may be better identified by local law enforcement in cooperation with the larger community. A good relationship that encourages communication between religious facility leaders and local law enforcement should facilitate the flow of information about potential threats to an institution from persons in the larger community.

3.1   Threat Assessments

The security practices ultimately developed should address the threats deemed most likely to occur or have the potential to result in the greatest damage. Potential threats to religious facilities can originate from disaffected individuals associated with the institution, but can also originate from outside the community. A threat assessment team may be staffed with a combination of facility personnel, members who attend services, mental health services, and emergency responders.

Threat assessment teams should consider engaging in a three-step process to evaluate a person(s) of concern.
- First, identify any individual(s) whose behavior may cause concern or disruption and that may affect members of the community.
- Second, assess whether the identified individual(s) possesses the intent and ability to carry out an attack against the institution or member of the institution, and if the individual has taken any steps to prepare for the attack.

- Finally, manage the threat posed by the individual, to include disrupting potential plans of attack, mitigating the risk, and implementing strategies to facilitate long-term resolution[5].

Although religious facility threat assessment teams may be less able to detect threats to the community which originate from individuals who are not affiliated with the facility, positive relationships with local law enforcement can facilitate information sharing and help facility personnel learn of potential threats that may originate from outside the facility. Since religious facilities may confront a variety of threats, a comprehensive strategy combining risk-informed prevention, protection, and preparedness activities, along with resilience enhancements will allow religious facilities to manage and mitigate the most serious threats to their safety and security.

3.2   Potential Attack Indicators

Attack indicators are observable behaviors that may precede an attack and may be detected as an individual prepares and plans for an attack. Indicators may include, but are not limited to: the perpetrator conducting surveillance, engaging in training, and/or beginning mobilization activities in advance of an attack. Potential indicators can be grouped into the following categories: individual behavior indicators, surveillance indicators, imminent attack indicators, and surrounding area indicators. Understanding behaviors that are unusual, concerning, or suspicious, as well as behaviors that may be indicative of surveillance or imminent attack are essential in the efforts to protect communities from threats of violence. It is important to note that multiple indicators may not represent suspicious or nefarious activity; context should be considered, but all indicators that are observed should be reported

3.2.1 Individual Behavior Indicators

Individuals who threaten to carry out some attack may engage in a number of behaviors that raise concern in others who know the individual. These behaviors should be looked at in the context of an individual's life and current situation, such that an individual who displays several of these concerning behaviors and is also dealing with a negative life event may be of concern and warrant some intervention[6].With respect to active shooter situations, investigations and analysis show that many active shooters were described as social isolates, harbored feelings of hate and anger, and/or had some reported contact with mental health professionals. Mental illness is commonly referenced as a potential contributing factor, but its causal impact on the attack can only be speculated. Common catalysts or triggers observed include: loss of significant relationships, changes in living arrangements, changes in financial status, loss of job, major adverse changes to life circumstances, and/or feelings of humiliation or rejection on the part of the shooter[7].

Some individual behavior indicators include:

---

[5] http://www.secretservice.gov/ntac/CampusAttacks041610.pdf
[6] http://www.secretservice.gov/ntac/ssi_final_report.pdf
[7] Joint Intelligence Brief – Recent Active Shooter Incidents Highlight Need for Continued Vigilance, 2012

- Socially isolated
- Threats of violence
- Unsolicited focus on dangerous weapons
- Unstable emotional responses
- Intense anger and hostility
- Loss of significant relationships
- Feeling either arrogant and supreme, or powerless
- Expressions of paranoia or depression
- Increased use of alcohol or drugs
- Depression or withdrawal
- Talk of suicide
- Increased absenteeism

3.2.2 Surveillance Indicators

Surveillance indicators may provide evidence that a religious facility is being monitored and/or assessed by individuals planning an attack. Indicators of potential surveillance include persons in the vicinity of religious facilities attempting to gather information about the facility, its operations, and/or its protective measures.

Some potential indicators that religious facilities may be under surveillance include:

Surveillance Indicators – Suspicious Persons
- Persons using or carrying video/camera/observation equipment 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 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.

3.2.3 Imminent Attack Indicators

These indicators may demonstrate 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. If an attack seems imminent and an immediate action is required, call 911 (local law enforcement) and follow all emergency operations plans.

Some potential indicators of an imminent attack include:

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 perimeter fence or gate, perimeter lighting, or other security device.

3.2.4 Surrounding Area Indicators

These 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 (generally identified by local law enforcement organizations) that may appear in the communities surrounding religious facilities that should be considered and factored into decisions regarding security. Religious facilities can 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.

Surrounding Areas 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 or unexpected maintenance activities (e.g., road repairs) near the facility.
- Sudden increases in power outages designed to test the backup systems or recovery times.

3.3 Protective Measures

As discussed earlier, the religious facility environment is managed by creating layers of protective measures in collaboration with community partners that allow religious institutions to deter, delay and detect threats. These sensors also allow an institution to consider a threat as soon as possible and to more effectively respond to, further deter, eliminate or mitigate that threat. Technological sensors such as surveillance cameras or alarms (fire, smoke, tornado, and intrusion detection) may inform decision making. Barriers, whether locked doors or bollards, and facility personnel should be utilized to delay a threat and afford more time for effective decision making. For example, a locked door creates time to better understand the situation and to make a better response decision. Pre-arranged responses to identified threats is also a mechanism to manage time during a crisis as a well-rehearsed response to a threat (e.g. fire drill) allows a more effective response under stress in minimal time.

As information is received during an emergency situation, a number of factors influence leaders' ability to make appropriate decisions. Time, or the lack of time, is a principle disrupter of effective decision making. Strategies to improve responses during a crisis should focus on time management. An effective security plan should expand the window of time available to leaders to make a good decision. A strong security plan will provide institution leaders opportunity and time during a crisis to make decisions about providing for the welfare of their community.

Protective measures that deter, delay, and detect threats include equipment, personnel, and procedures designed to protect a facility against threats and 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. Some are applicable to a wide range of facilities and against a number of threat streams, whereas 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. Some protective measures are 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 members are involved. Including all employees and members 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 (ECIP) Program, protective measures employed by religious facilities, actions taken 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 surveillance cameras. Effort also has been expended on reducing dependencies on critical products, transportation, and information technology. Refer to Appendix 1 to view a baseline security practices checklist.

3.4   Reporting Procedures

The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) is one of our best defenses against attacks and our greatest resource to building capacity to deter threats. To benefit from a SAR, create a common reporting system and develop guidance for facility personnel and members to report suspicious activity to their religious facility as well as appropriate local law enforcement agencies. Also consider creating an anonymous way for people to report suspicious activity. In addition, it is critical that law enforcement officers at all levels of government – state, local, tribal, territorial (SLTT), and Federal – who observe suspicious behaviors or receive reports from concerned civilians, private security, and other government agencies share information with state and major urban area fusion centers, the FBI, and other law enforcement agencies to help prevent future attacks from occurring.

4 Preparedness

Effective crisis planning begins with leadership at the top. Every governor, mayor, legislator, and religious facility leader should work together to make crisis planning a priority. Top leadership helps set the policy agenda, secure funds, and brings the necessary people together across

agencies. Participation of leaders at the grassroots level is also critical because they will help inform the religious community of the planning process. Moreover, religious facilities should open the channels of communication well before an emergency incident. Relationships need to be built in advance so emergency responders are familiar with an institution's facilities. Effective emergency management builds from close collaboration, coordination, and communication between religious facilities, mental health officials, traditional first responders (e.g., law enforcement, fire officials), and numerous other partners in the community. It is important for religious facility leadership to cultivate a relationship with city emergency managers, public works officials, and mental health professionals sooner, rather than later. Emergency operations plans should be developed in partnership with other community groups as well, including law enforcement, fire safety officials, and emergency medical services. These groups have already developed emergency operations plans and can be helpful in the development of religious facility plans. All religious institutions should create a planning team whose key function is to identify the types of crises that may occur within institution facilities and define what events would activate the emergency operations plan. The team may consider many factors such as the institution's ability to handle a situation with internal resources and its experience in responding to past events[8].

4.1   Establishing Collaborative Planning Teams

The process of developing and maintaining an emergency operations plan is complex; therefore, before a plan is developed, collaborative planning teams should be assembled. These teams are composed of a variety of professionals with expertise in emergency management (e.g., police, fire and emergency medical services personnel) and include community partners (e.g., public and mental health professionals) and religious facility leadership. Collaborative planning teams should be responsible for: establishing relationships with community partners; coordinating vulnerability assessments; developing training activities and conducting exercises to support and improve the emergency operations plan; and establishing and enforcing a religious facilities emergency operations plan. The Departments of Education, Health and Human Services, Homeland Security and Justice have developed a comprehensive resource, *Emergency Operations Planning for Houses of Worship,* to facilitate developing an emergency operations plan.[9]

4.2   Creating an Emergency Operations Plan

Knowing what to do when faced with a crisis can be the difference between calm and chaos, between courage and fear, and between life and death[10]. To best prepare your staff, members, and possible visitors for a crisis, create an Emergency Operations Plan (EOP), and conduct training exercises. Together, the EOP and training exercises will prepare your staff and members to effectively respond to an incident and help minimize loss of life. Facility readiness requires that leadership develop and exercise response plans that apply general preparedness and response protocols to specific types of emergencies and facility capabilities (including security resources). EOPs need to be customized to communities and facilities to meet the unique needs of a specific

---

[8] http://www2.ed.gov/admins/lead/safety/emergencyplan/crisisplanning.pdf
[9] Add link when it is identified
[10] http://www2.ed.gov/admins/lead/safety/emergencyplan/crisisplanning.pdf

religious facility. Religious facility specific EOPs should consider predetermined perimeters, plans to create a command post during an incident, media liaisons, a Joint Information Center (JIC), police staging areas, and alternative sites for evacuation. Additionally, it is incredibly important to review, update, and practice the EOP regularly. Good plans are never finished; they can always be updated based on experience, research, and changing vulnerabilities or threats.

4.2.1 Define Roles and Responsibilities

Define roles and responsibilities of religious facility staff as well as community partners. Define what should happen, when, and at whose direction—that is, create an organizational system. The organizational system should involve much of the institution's staff and faculty; important tasks will be neglected if one person is responsible for too many functions. Institution staff could be assigned roles based on their skills and using the Incident Command System (ICS) put forth in the National Incident Management System (NIMS) such as: institution commander, public information office, safety officer, and liaison officer. Both individuals and backups should be assigned to these roles. Many institutions and emergency responders use the ICS, to manage incidents. ICS provides a structured way for delegating responsibilities among institution officials and all emergency responders during crisis response[11]. Also, it is important to be aware of roles that outside agencies play, the responsibilities they will assume, and how they will interact with religious facility staff, members, and visitors. It is especially important to determine who will communicate with families and the community during an incident and how they will communicate. A Joint Information Center (JIC), where information sharing is centralized, should be created. This will support media requests (e.g., request for press conferences) and provide a single, accurate outlet for information.

4.2.2 Notification Procedures

One of the first steps in planning is developing a mechanism to notify members and religious facility personnel that an incident is occurring and to instruct them on what to do. There should be specific methods for communicating an incident internally to staff, members, and facility visitors and separate methods for communicating an incident externally to media, families, neighbors, and the community. Methods of communication should be implemented based on the unique needs of each religious facility or community.

4.2.3 Evacuation, Lockdown, and Shelter-In-Place Policies and Procedures

When an incident occurs, quickly determine whether facility personnel and facility occupants need to be evacuated, locked down or assume shelter in place. Evacuation requires all occupants to leave the building. While evacuating to the facility parking lot makes sense for a fire drill that only lasts a few minutes, it may not be an appropriate location for a longer period of time. The evacuation plan should include backup buildings to serve as emergency shelters, such as nearby community centers, businesses, or schools. Evacuation plans should include contingencies for weather conditions. Evacuation procedures should include a special triage area if the situation requires it.

---

[11] http://www.fema.gov/incident-command-system

Lockdowns are called for when a crisis occurs outside of the facility and an evacuation would be dangerous (e.g., escaped criminal). A lockdown may also be called for when there is a crisis inside and movement within the facility will put facility occupants in jeopardy. All exterior doors are locked and occupants stay in an enclosed area. Windows may need to be covered.

Shelter-in-place requires staff, members, and visitors to immediately find a room with no or few windows, and take refuge there. All windows, exterior doors, and other openings to the outside should be closed and locked. Additionally, all fans, heating and air conditioning systems should be turned off if possible to prevent any materials or agents from circulating through ventilation systems.

Active shooter situations are unpredictable and evolve quickly. Because active shooter situations are often over within 10 to 15 minutes, before law enforcement arrives on the scene, individuals must be prepared both mentally and physically to deal with an active shooter situation. In the event of an active shooter situation, it is imperative to quickly determine the most reasonable way to protect your own life. If there is an accessible escape path, attempt to evacuate the premises. If evacuation is not possible, find a place to hide where the active shooter is less likely to find you. As a last resort, and only when your life is in imminent danger, attempt to disrupt and/or incapacitate the active shooter.[12]

4.2.4　Plans for Diverse Needs of Children and Staff

Emergency actions plans should provide for the needs of facility personnel, members, and visitors with disabilities and other functional and access needs. This is especially important when considering evacuation procedures. Predetermined evacuation routes and staging areas for those with disabilities should be considered.

4.2.5　Consider Necessary Equipment and Supplies

Provide staff with the necessary equipment to respond to a crisis. Consider whether there are enough master keys for emergency responders so that they have complete access to the facility. Ensure that phones or radios necessary for communication are available and ready for use. Redundancy is important; consider a second telephone service that is available to allow communications in the event of an incident. Maintain a cache of first aid supplies and have them dispersed throughout different rooms. Ensure that any emergency generators have been regularly inspected and are in working condition. Emergency generators can be relied upon to provide emergency lighting in otherwise dark areas, as well as power up communication devices during and after an incident

4.2.6　Common Vocabulary

It is critical that religious facility personnel and emergency responders know each other's terminology. Work with emergency responders to develop a common vocabulary. The words used to give directions for evacuation, lockdown, and other actions should be clear and not hazard specific. The Federal Emergency Management Agency (FEMA) recommends using plain

---

[12] http://www.dhs.gov/xlibrary/assets/active_shooter_booklet.pdf

language to announce the need for action, for example, "evacuate" rather than "code blue." Plain language allows everyone in the school building including new visitors to understand what type of response is requested.

4.2.7 Accountability System

As soon as a crisis is recognized, it is important to account for all facility personnel, facility members, and visitors. Emergency responders treat a situation very differently when people are missing.

4.2.8 Communication with External Entities

It is important to address how the religious facility will communicate with all of the individuals who are directly or indirectly involved in the crisis. Plan how to communicate with families, community members, and the media. Consider writing template letters and press releases in advance so personnel will not have to compose them during the confusion and chaos of an incident.

4.2.9 Emergency Drills

Preparedness includes emergency drills and crisis exercises for facility personnel, members, and emergency responders. Many religious facilities have found Tabletop Exercises (TTX) very useful in practicing and testing the procedures outlined in their emergency operations plan. Training and drills can help identify issues and problems that need to be addressed in the emergency operations plan.

5 Response

A crisis is the time to follow the emergency operations plan, not to make a plan from scratch. This section provides broad action lists for religious facility personnel, staff, and members. During a crisis, leaders need to project a calm, confident, and serious attitude to assure people of the seriousness of the situation and the wisdom of the directions being given. It is also important to communicate accurate and appropriate information. Use the channels of communication identified in the emergency operations plan.

5.1 Religious Facility Leadership

Action List for Evacuation – Religious Facility Leadership
o   Determine whether a crisis exists and if so, the type of crisis, the location of the crisis, and the magnitude of the crisis.
o   Notify appropriate emergency responders.
o   Follow evacuation procedures and quickly exit building to designated evacuation location.
o   Consolidate accountability information.
o   Communicate with emergency responders and facility staff and members.
O   Communicate with appointed public liaison.

o   Determine whether a crisis exists and if so, the type of crisis, the location of the crisis, and the magnitude of the crisis.
o   Notify appropriate emergency responders.
o   Follow lockdown procedures and provide oversight of entire lockdown.
o   Consolidate accountability information.
o   Communicate with emergency responders and facility staff and members.
o   Communicate with appointed public liaison.

5.2   Religious Facility Staff and Members

Action List for Evacuation – Staff and Members (janitorial staff, administrative staff, etc.)

o   Determine whether a crisis exists and if so, the type of crisis, the location of the crisis, and the magnitude of the crisis.
o   Notify appropriate emergency responders.
o   Notify administrative staff so all facility occupants can be notified of incident.
o   Follow evacuation procedures and quickly exit building to designated evacuation location.
o   Provide support where needed (direct occupant traffic, provide medical support, etc.).

Action List for Lockdown – Staff and Members (janitorial staff, administrative staff, etc.)

o   Determine whether a crisis exists and if so, the type of crisis, the location of the crisis, and the magnitude of the crisis.
o   Notify appropriate emergency responders.
o   Notify administrative staff so all facility occupants can be notified of incident.
o   Follow lock down procedures.
o   Provide support where needed (direct occupant traffic, provide medical support, etc.).

6   Recovery

The goal of recovery is to return to normal operations and restore the infrastructure of the facility as quickly as possible. Focus on members and take as much time as needed for recovery. Religious facility staff can be trained to deal with the emotional impact of a crisis, as well as to initially assess the emotional needs of members, staff, and responders. One of the major goals of recovery is to provide a caring and supporting environment.

6.1   Assemble a Crisis Intervention Team and Assess Emotional Needs of Staff, Members, Facilities, and Responders

A Crisis Intervention Team (CIT) is comprised of individuals assessing and responding to individual's emotional needs in the aftermath of an incident. Service providers in the community may want to assist after a crisis. With prior planning, those with appropriate skills and certifications may be tapped to assist in recovery. Assess the emotional needs of all members and staff, and determine those who need intervention by a counselor, social worker, psychologist, or

other mental health professional. In addition, available services need to be identified for families, who may want to seek treatment for their children themselves.

6.2   Keep Members, Families and the Media Informed

Be clear about what steps have been taken to attend to member safety after the crisis has occurred. Let families and other community members know what support services the facility are providing or what other community resources are available. This information sharing should run through an institution's public affairs office.

6.3   Provide Stress Management

Allow members to talk about what they felt and experienced during the traumatic event. Younger children who may not be able to fully express their feelings verbally will benefit from participating in creative activities, including drawing, painting, or writing stories. Engage older adolescents in group discussion, and address any issues of guilt. Additionally, provide on-site counselors for a minimum of one week after the incident.

6.4   Restore Infrastructure

Restoring infrastructure is essential to the restoration of a positive, nurturing, and safe facility environment. Restoring damaged infrastructure after an emergency incident is a positive, tangible, sign of recovery for members and staff. Restoring infrastructure after an incident provides an opportunity to evaluate incident response and implement new and effective protective measures if necessary.

6.5   Evaluate

Evaluating recovery efforts will help prepare for the next crisis. Use several methods to evaluate recovery efforts. Conduct brief interviews with emergency responders, members, staff, institution officials, and other affected community members. Focus groups may also be helpful in obtaining candid information about recovery efforts. Evaluate what worked, what did not, and how operations or emergency operations plans can be improved. Update and strengthen the emergency operations plan so that in a crisis, no one is left behind. It may also be prudent to conduct a community briefing within 48 hours of the incident. Additionally, it may be helpful to conduct after action reports with institution personnel and first responder commanders within one week of the incident.

Additional Resources

U.S. Secret Service National Threat Assessment Center (NTAC)
http://www.secretservice.gov/ntac.shtml

Progress Report on the President's Executive Actions to Reduce Gun Violence
http://www.dhs.gov/publication/progress-report-president%E2%80%99s-executive-actions-reduce-gun-violence

Active Shooter Preparedness
http://www.dhs.gov/active-shooter-preparedness

Training First Responders and School Officials on Active Shooter Situations
http://www.dhs.gov/sites/default/files/publications/fact-sheet-training-first-responders_0.pdf

Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)
http://nsi.ncirc.gov/

If You See Something, Say Something
http://www.dhs.gov/if-you-see-something-say-something-campaign

FEMA: Prepare. Plan. Stay Informed
http://www.ready.gov/

President's Plan to Protect our Children and Our Communities by Reducing Gun Violence
http://www.whitehouse.gov/sites/default/files/docs/wh_now_is_the_time_full.pdf

DHS Protective Security Advisors
http://www.dhs.gov/protective-security-advisors

Critical Infrastructure Vulnerability Assessments
http://www.dhs.gov/critical-infrastructure-vulnerability-assessments

Photo Sources

Picture 1: Caliendo, Marilee. FEMA Photographer. Morning View, Kentucky. March 16, 2012. http://www.fema.gov/photodata/original/55809.jpg .

Picture 2: Henshall, Greg. FEMA Photographer. New Orleasn, LA. January 7, 2006. http://www.fema.gov/photodata/original/21080.jpg.

Picture 3: Dubrowa, Adam. FEMA Photographer. Pleasant Grove, Alabama. May 1, 2011. http://www.fema.gov/photodata/original/46822.jpg.