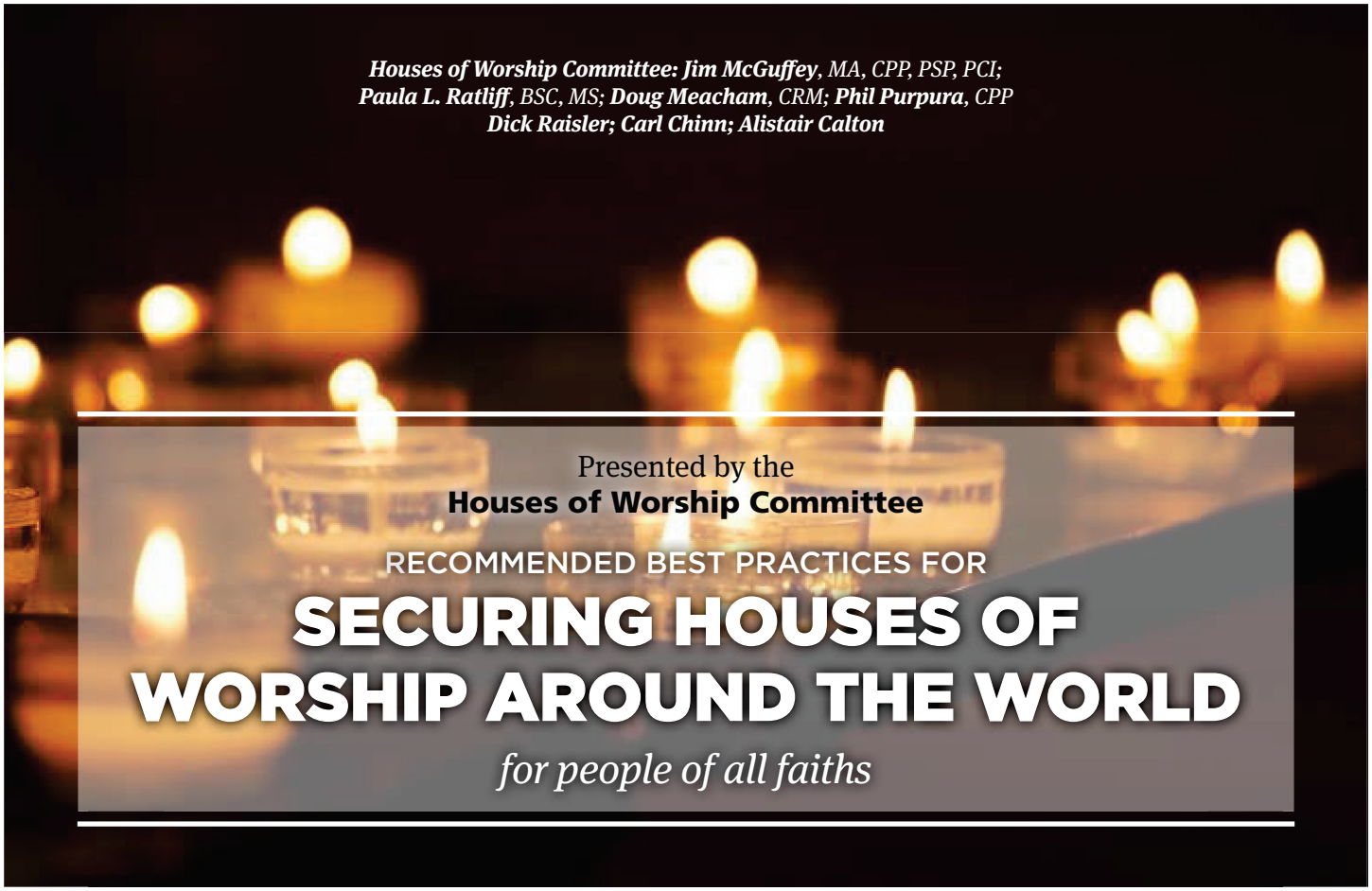
***Houses of Worship Committee: Jim McGuffey**, MA, CPP, PSP, PCI;*
***Paula L. Ratliff**, BSC, MS; **Doug Meacham**, CRM; **Phil Purpura**, CPP*
Dick Raisler; Carl Chinn; Alistair Calton



Presented by the
Houses of Worship Committee

RECOMMENDED BEST PRACTICES FOR

SECURING HOUSES OF WORSHIP AROUND THE WORLD

for people of all faiths

Securing Houses of Worship Around the World

Security and worship can be successfully blended for those who worship in your facility. No house of worship (HOW), whether a church, mosque, temple, or synagogue is exempt from crime, whether committed by an internal member, a stranger, or as a random act of terrorism. We must consider threats and be ready to respond in a quick, efficient, and effective manner.

The security of HOWs encompass many components, such as the safety of the congregation or any individual who attends a service or a program, preservation of religious artifacts, protection of fiscal assets and cyber information, medical emergencies, natural disasters and/or acts of terror. HOWs are also serving as places of refuge for persons fleeing religious persecution from locations around the world.

Each congregation is tasked with the challenge of creating a safe place to worship. Various security precautions can be implemented in a non-intrusive manner, completely unknown and unobserved by congregants. For example, implementing a "Welcoming Committee" that includes individuals observing and welcoming people as they enter the facility will basically be unnoticed as a security program, yet it is highly effective when the members are trained in security detection.

Other security measures may appear drastic in some settings, while rather routine in others. For example, the church bombings in Tanta and Alexandria, Egypt, in April 2017, highlighted the importance of body scanners, as one of the bombers was denied access to the church until he had walked through the scanner. He detonated the bomb as he approached the scanner, killing several and injuring many. An important point here is that because the bomber was denied entrance due to access control, many lives were saved. HOWs in most countries must consider the possibility of terrorism from bombs, vehicles, or other means.

Religious leaders are essential to the successful implementation of security programs and, in many instances, will be the ones to take the lead. If your congregation includes security and/or law enforcement professionals or military personnel, you may have additional support in your initiatives. Regardless of congregation size, facility size, or location, it is imperative that religious organizations keep the topic of security on their radar screen.

ASIS INTERNATIONAL® | Cultural Properties Council

Religious facilities around the world vary greatly in size and resources, resulting in a diverse commitment to security. Some assemblies may be held in a home or a community center, while other facilities are huge campuses with multiple buildings and activities occurring around the clock. Each facility will have different considerations.

For example, a small congregation of 100 will have a different list of concerns than a congregation of 1,000. However, it is imperative that each congregation strive to enhance its level of security and determine what is appropriate for their facility. On June 17, 20015, when a 21-year-old shooter entered the Emanuel African Methodist Episcopal Church in Charleston, South Carolina, he chose a location with only twelve witnesses. Yet, when a pedophile is looking for a victim, he may look for a larger congregation where it is easy to slide right in, unnoticed and unobserved.

A synagogue in Jerusalem will have different levels of threats than a synagogue in the United States, yet each face various threats on many different levels. The Anti-Defamation League reported in January 2017 that threats have increased, particularly bomb threats to facilities and that there has been a rise in anti-Semitic assaults on college campuses. It is imperative that security is included in the HOW budget and as an agenda item in business meetings. Many security recommendations listed in this paper can be implemented at little or no cost. On the other hand, some can be extremely expensive. This white paper cites a few best practices for consideration. Size, location, and available resources will influence the recommendations and best practices that are implemented.

Security should be a component of every event that is offered at your facility, whether a prayer service, a youth event, or a concert. To reduce and/or eliminate threats, consideration must be given to the event, attendance, logistics, times (e.g., what are the challenges of night programs versus day programs?). What are the potential threats and what can be done to reduce and/or eliminate the threats?

As leadership supports the issue of security, the first step is to develop a security plan for your facility based on the premise that it will be an evolving document that will change frequently. Getting started and putting security on your radar screen is essential to providing a safe place to worship.

The Houses of Worship Committee developed this paper to assist religious leaders and security professionals in the development of a security plan. An earlier version of this document was published in 2012. It was revised in 2017 to address threats from terrorist organizations such as ISIS that has affiliated itself with Boko Haram to focus solely on Christian churches, specifically citing Christian HOWs in the U.S., England, France, and other western countries. This is of significant concern as terrorists are instructing disenchanted individuals, also known as "lone wolves," not to wait for assistance or formal instruction, but to begin attacking using knives, vehicles, or whatever means to harm others. Domestic or homegrown terrorism also is of major concern to our way of life and worship.

This paper is divided into three sections:

- Interior security
- Exterior security
- Procedural and/or best practices

This is not an all-inclusive list, but a summary of the highlights to review and consider as you develop a security plan for your facility. Additionally, ASIS International has various resources to assist you in this process, including a book by committee member, Paula L. Ratliff, entitled **Crime Prevention for Houses of Worship, 2nd edition**. Please review the ASIS website for additional resources: *asisonline.org*

Interior Security Controls

Access Control

Controlling and limiting access is one of the most important steps that can be taken to improve security, and should be implemented whenever possible. Some HOW staff and worshippers will not be comfortable with restricting access, however. If this is the case, then it is important to monitor access of those in attendance and those outside the premises.

- Doors and windows should be secured when the building is vacant.
- Limit points of access. When opening your facility, consider the event, the number of people, and the location of the event. Limit access by only opening doors that are close to the area being used. Do not open every door.
- Establish checkpoints based on need--and staff accordingly. A checkpoint is an entry where all people and things are screened based upon the security plan for the current threat environment.
- Zone areas in large facilities based upon activity and establish access based upon need (e.g., access to sanctuary much different than business offices or childcare rooms).
- Consider key-code entry systems for areas such as gyms.
- Reduce access points to bare minimum while maintaining fire code compliance.
- Limit access to childcare, business offices, cash counting area, and media rooms.
- Establish policies to maintain access control.

- ✓ Reduce opportunities for just one person to be alone in the HOW.
- ✓ If a limited number of people are in attendance for an event, lock the doors when the event starts.
- ✓ Establish greeters or a welcoming committee to watch the doors. These individuals will be trained on how to interact with a suspicious person and whom to contact. Consider a visitors and guest's authentication procedure.
- ✓ Establish someone to "patrol" the halls, classrooms, and restrooms on a random basis.

- Have members stand at each entrance to the area of worship. They should observe, meet, and greet every person entering. This would be the second layer of security, the first being the welcoming committee members who are observing people as they enter from the outside.

Alarm System

- Install a basic burglar and fire alarm system.
- Ensure adequate fire alarm coverage. The local fire department can help with determining what is needed for your facility.
- Ensure an alarm system covers access points and key areas where expensive items are housed.
- Use a reliable monitoring vendor and ensure contact information remains current.
- Develop a policy that addresses response to alarms.
- A Camera system can also serve as an alarm system by using video analytics and integrating with access control systems.
- Install panic alarms at public reception areas where employees can initiate emergency procedures when suspicious persons approach and request access.

CCTV System

- Camera coverage should be considered for critical areas (such as areas with children, the business office, the clergy's office, etc.) and access points. They can also be focused around items that are most likely to be stolen. For places of worship with little capital to spend, a camera with audio that can be monitored from a cell phone may be purchased for about $200.

Childcare/Daycare Areas

These areas require additional security measures.

- Cameras should capture every door and point of entry. Additionally, cameras should be in the infant care rooms, daycare rooms, and areas where children play/eat/etc.
- All doors into daycare rooms or play areas should have windows so that no adult is ever concealed from view while supervising children.
- If cameras are installed in daycare centers, inform parents and caretakers that you would be storing digital data of their children.
- These areas must have sufficient staff and exceptional policies and procedures to ensure the children are safe from internal and external threats. A very serious potential mistake would be to release a child to the wrong person, which could happen during a divorce or with a blended family.
- Staff, child, and family identification cards can assist in controlling access and be integrated in card access control systems. They also assist in reunification procedures after an incident.
- Many local government offices provide children's safeguarding support. If you are not aware of how to access this, then speak with local school staff who will provide you with advice on safeguarding the welfare of children in your premises.

Computers

- Cybercrime has become a global threat. The Insurance Information Institute reports that "the 2017 Identity Fraud Study, released by Javelin Strategy & Research, found that $16 billion was stolen from 15.4 million U.S. consumers in 2016, compared with $15.3 billion and $13.1 million victims a year earlier."
- Ensure passwords are protected.
- Back up information daily.
- Use virus and malware protection.
- Ensure computers are secured when not in use.

- Always install the latest patches and updates when prompted. This mitigates many hacking programs that rely on outdated vulnerabilities in your software. Set your computer to auto install updates.

Doors

- Ideally doors should be wood or steel with a solid frame. However, many HOWs have glass doors to allow visibility. In that case, purchase the thickest glass you can afford.
- Hinge pins should be located on the interior of door, or capped, if on the outside to prevent easy removal.
- Consider anti-intrusion glass film for entry doors and other ground level glass.

Windows

- Ensure that windows are secured prior to closing and latches are in working order.
- If windows are opened for air circulation, only open windows that are monitored and/or located where people cannot climb through.
- Consider glass liner for public areas to reduce and prevent glass chards for weather or explosions that may cause breakage and dispersion.

Locks and Keys

A code entry system with an alarm provides two levels of protection. The key code can indicate when someone enters and an alarm system will indicate if a door is unlocked. Additionally, consider mechanical locking systems, as they have become more affordable.

- Regularly check the locks on the doors and windows for evidence of tampering.
- If standard locks are used, keys should be issued to individuals who have a specific need. Maintain a master key list and require recipients to sign a receipt for keys.
- Keys for critical areas and master keys must be especially controlled.

Exterior Security Controls

Exterior security controls encourage us to think about how best to secure the perimeter of the church, parking lots, playground areas, and mass drop-off areas. Think critically about the vulnerability of crowds and how they can be attacked, both outside and inside buildings. In a 15-year study of the most violent crimes at faith-based organizations, more than 70% of the acts occurred outside the building on ministry grounds or parking lots.

The Perimeter

- Consider enhancing perimeter security with fencing or crime prevention through environmental design (CPTED) principles. Consider enhancing perimeter security by adding a decorative fence-- whether aluminum, board, stone, brick and/or multiple combinations thereof. The goal is to clearly define the church perimeter and limit and/or reduce the potential for people to drive across the property.
- Install planter barriers and gates near entrances.
- Secure points of entry when no events are taking place. If your facility has back entrances and parking lots, these should be locked off.
- Trim shrubs/bushes/trees that are near the building to reduce hiding places.
- Remove potential fire hazards, such as trash and debris. Keep dumpsters in a locked dumpster pad.
- Consider vehicle barriers and/or bollards for vulnerable entries, special events, or in case of a terrorist threat when stand-off distance is required for vehicles. Barriers can be as simple as strategic parking of staff vehicles or as complex as a built-in place.
- Identify exterior hiding places, equipment vulnerabilities, utilities entries/shutoffs, fire department connections and hydrants. Check them for signs of activity before any event.
- Utilize CPTED principles where applicable, (i.e. natural berms coupled with plants, trees, and rock formations to provide perimeter security that would mitigate vehicle access to property). Incorporate steps, curbs, and trees near checkpoints that would prevent vehicle or similar type attacks. Install secured and anchored benches, bollards, or planters to enhance middle perimeter security.

- Research and study local ordinances to learn of restrictions and guidance on fences, lighting, foliage, signs, protests, noise, and merging private/public vehicle flow. Related to this, know your property lines.

Exterior Lighting

- Lights should be placed on all doors and windows. Motion detector lights should be considered for doors and windows. Ensure all lights are in working order.
- Lights should be on from dust to dawn. Consider lights with solar panels as this may reduce the cost of the energy.
- Install lights in the parking lots, ball fields, and playground areas.

Parking Lots

- Larger facilities may need an officer to direct traffic. This will ensure timely entry and parking. The officer(s) can patrol the parking lots during the services. This task can also be completed by members of your "security team." Outfit them in high-visibility vests and radios.
- Develop a facility traffic pattern which allows for expedited parking and retains an entry route and staging area.
- Buffer parking areas from sanctuary where possible. Buffers can be fences, landscaping, architectural features, plant barriers.
- Keep parking lots lighted at night, and if fenced and gated, close them.

CCTV System

- Camera coverage is recommended for the exterior of the facility. Every area from the entrances to the parking lots should be covered. Some cameras only record when motion is detected, others record 24-7. Cameras can be monitored from the inside by your security team members and remotely on hand held devices as needed or based upon analytics, as mentioned above.
- If you are gathering quotes from companies about new cameras, think about what you want to achieve with them. If they are only for monitoring or identifying activity, then medium to low resolution camera will be much less expensive and still do the job.

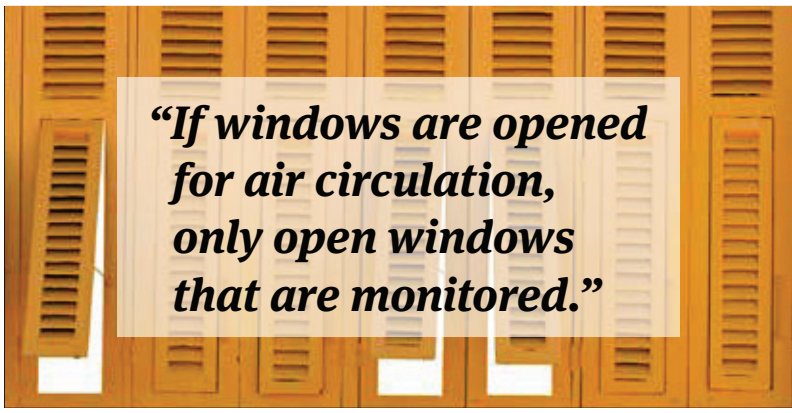
Procedural Recommendations and Best Practices

Designate "security" as a priority and commit to developing a security plan.

- Form a security committee that includes religious leaders, congregants, security professionals, law enforcement, medical professionals, and others in your planning process.
- Designate "security" as a ministry and recruit members to serve.
- Appoint a "security leader" to oversee the development and implementation of the security plan. Schedule regular meetings to review procedures and incidents.
- Coordinate safety and security planning with the special event planning committee.

Foster relationships with your local law enforcement agencies.

- Invite local, state, and federal law enforcement to your house of worship. Offer your building and parking lots as places to visit. Offer your facility as a training location for local police S.W.A.T. members. This gets them familiar with the facility in the event of an emergency.
- Ask for assistance with traffic control.
- Initiate contact with local law enforcement to create a contact list of e-mails and phone numbers so that you know whom to contact.
- Include law enforcement in your security planning process.
- Notify law enforcement of schedules and special events.
- Consider hiring off-duty police officers as part of your security program.
- Coordinate with law enforcement to conduct security surveys, risk assessments, and threat assessments of your facilities and neighboring areas.



Develop and/or attend security related training for your security committee members.

- Develop a "Welcoming Committee" of individuals and/or ushers who are trained in security detection and emergency responses.
- Conduct evacuation drills with staff and volunteers.
- Provide training on how to respond to medical emergencies.

- Plan and practice scenario based response procedures identifying suspicious behavior, handling a threatening situation, evacuations and lockdowns. Train employees and volunteers about letter bombs and improvised explosive devices (IEDs). Ensure they have quick access to a bomb threat form.
- Attend firearms training if your committee recommends that individuals are armed during services and special events.
- Attend training on how to recognize and deal with individuals with mental illness and substance abuse issues. Many "lone wolf" terrorists may have mental health problems and/or social conditions that have contributed to their terrorist sympathies. While this does not mean we should judge people with mental health conditions as a threat, we should take time to train on how to engage people suffering from a mental health crisis or someone who has an Autism Spectrum Disorder (ASD) condition which may mean normal communication methods would fail.
- Attend and offer training for victims of domestic violence and encourage them to report any suspicious of violence from their estranged partner.

Develop a security plan that includes the following components, as appropriate for your congregation. *(This is not an all- inclusive list. Please consult additional resources.)*

- Internal controls – focuses on security inside the facility. See above.
- External controls – focuses on security outside of the facility. See above.
- Emergency plan for medical emergencies, fires, natural disasters, and acts of violence
- Communication, crisis management and media procedures
- Financial and cybersecurity
- Hiring procedures, background and financial checks
- Camera surveillance and monitoring
- Daycare, school and youth security
- Traffic control, fleet management, and driving credentials
- Insurance, inventory, and artifacts
- Shelter-in-place/lockdown procedures
- Investigations, reporting, and evidence procedures
- Special event safety and security plan
- Off-site excursions and events
- Opening, locking, and closing procedures
- Benevolence and other outreaches
- Foreign mission trips

Emergency Plan for Medical Emergencies, Fires, Natural Disasters, and Acts of Violence

- Plan for events that could happen in your facility and those that could happen in your community. Offer your facility as a staging location or emergency shelter.
- Designate an area for medical emergencies and ensure that the room is equipped with emergency medical kits, defibrillators, and, if having a large event, consider having an ambulance on the property. It is recommended to have items such as flashlights, blankets, and emergency phones available in case of mass casualties.
- Place your first aid kits in different locations around the building. In the event of a major incident, some parts of the building may be unusable due to fire or damage.
- Ensure that your volunteers have been trained in handling medical emergencies.
- Practice fire drills and teach the procedures to "shelter-in-place."
- Prepare your committee members for dealing with mass casualty events such as an active shooter, terrorist, or a natural disaster.
- Ensure all staff and volunteers are advised on the safe communication distances for electronic devices in the proximity of bombs or suspect devices (minimum 15 meters); the safe evacuation distance for a bomb (25 meters for a hold all, 100 meters for a car, and 400 meters for a truck).
- Develop a reunification plan for children who are relocated during emergency evacuations and train parents or guardians on the procedures and relocations sites.

Communication, Crisis Management, and Media Procedures

- Develop a list of emergency contacts to include law enforcement, religious leaders, relevant volunteers, security committee members, and others. Include phone numbers and all forms of social media contacts.
- Establish emergency communication protocols to clearly designate the chain of command as to who should be contacted in the event of an emergency and/or major incident.
- Designate a spokesperson for the congregation and stipulate that others refrain from speaking to the media. The spokesperson will gather the facts and issue statements with local law enforcement.

- Ensure that individuals' privacy is protected.
- Develop a plan for crisis management.
- Maintain as much control as possible to protect the innocent and ensure that families are notified prior to issuing statements to the media.
- Coordinate communication procedures that include mass notification texts, tweets, emails, and/or intercom.
- Regularly search social media for mention of your premises, religious leaders, or HOW. It is useful to monitor who is talking about you, but also if people posts accidentally divulge information. One example is a video with someone in the background typing in a key-code entry number. You can set auto alerts on most internet search engines.

Financial and Cybersecurity

- Ensure that individuals with access to money, checks, credit cards, and computers are carefully screened with a thorough background check and a credit report. Additionally, they should sign a confidentiality agreement stating that they will not copy, photograph, remove and/or release any data from the computers or other records.
- Keep cash in an adequate safe.
- Establish financial management procedures that include multiple persons handling the money with monthly reconciliations, internal reviews and audits. Require multiple signatures on checks and keep accurate records of expenditures.
- Submit financial reconciliations to leaders for review monthly.
- Develop procedures for cyber security which addresses password protection, daily backups, virus, and malware protection.

Hiring Procedures, Background, and Financial Checks

- Conduct background checks to include criminal and prior employment for paid or volunteer members, especially for those working with children. Individuals who handle money should consent to a credit and background check. Additionally, individuals who drive vehicles should have a license check. These checks should be updated on a regular basis.
- Before accepting new members, conduct a background investigation into their previous congregation to ensure there were no problems. Likewise, a review of social media accounts is recommended.
- Keep personnel files on all staff and volunteers. Establish a "wait time" when a new person arrives before allowing them to serve in various capacities, such as a nursery.

Camera Surveillance and Monitoring

- Install as many cameras as possible in your building. At a minimum, include entrances and exits and any areas where children may congregate. Additionally, if your facility has a gym or playground area, these should also be monitored via cameras. The goal is 360 degrees of coverage around buildings to include all entrances and exits.
- Install cameras outside of your building focusing on entrances and exits.

Daycare, School, and Youth Security

- Ensure that all volunteers and workers have a background investigation before working with children and/or youth.
- Develop policies for childcare check-in, check-out. A numbering system can remove the potential for an unauthorized pick up.
- Enforce the "rule of two": no one person accompanies a child to the restroom, nor is one person ever alone with a child.
- If your campus includes a daycare or school, develop specific strategies for securing youth areas and controlling and monitoring those who enter.
- Off-site events must be carefully monitored to provide a secure environment.
- Gyms, playgrounds, and sports fields present a separate set of challenges and must be addressed by your security committee.

Traffic Control, Fleet Management, and Driving Credentials

- Contact local law enforcement for assistance with traffic control before, after, and during services. If they cannot assist, consider hiring a security officer and/or crossing guard for any locations that could be dangerous for either walkers or drivers.
- Designate someone to maintain fleet records including maintenance and inspections. Avoid parking buses and vans in a manner where someone could hide between them and place an explosive device.
- Ensure that any person who operates a vehicle has a valid driver's license and a good driving record. These records must be monitored consistently. Drivers may need to be listed on your insurance policy.

Insurance, Inventory, and Artifacts

- Ensure that your facility is adequately insured for acts of vandalism, burglary, fire, terrorism, cybercrimes, and embezzlement.
- Maintain an inventory list and take pictures of anything of value, such as musical instruments, sound equipment, and artifacts. Include make, model, and serial numbers. These will be required in the event of a burglary or fire. Store records off-site and update on an annual basis.
- If your facility includes stained glass windows, it is recommended that they be covered with a wire mesh to reduce the potential for breakage.

Shelter-in-Place/Lockdown Procedures

- Train your volunteers and workers what to do if they witness or suspect an attack.
- Train your volunteers and workers on how to "shelter-in-place" and maintain a lockdown setting until the all clear is given.
- Train your volunteers and workers to secure the door and cover the windows, if possible. Take shelter in a closet, under a desk, or wherever cover is available. Never walk toward the sounds of gunfire or go out to investigate until the "all clear" signal is given.

Investigations, Reporting, and Evidence Procedures

- When a crime is reported, you should have clear guidelines as to how to respond. For example, any type of sexual assault or accusation should be reported to local law enforcement. Think immediately about the crime scene. Secure the area until law enforcement arrives.
- We encourage that all crimes be reported to the police. Otherwise, it is "swept under the prayer mat" and no one is enlightened as to the mode of operation, and the deviant may find another congregation to offend.
- Make appropriate changes/maintenance/enhancements of problematic areas. If a crime occurs in a specific location, changes should be made to reduce the opportunity.
- Review emergency response procedures, (i.e., lockdowns and evacuations) after an incident to assess what worked and what needs improvement.
- Document descriptions of suspicious people or vehicles.

Special Event Safety and Security Plan

- When having a concert or large gathering, consider hiring extra security to secure the building and parking lot and to provide traffic control.
- If having an event that lasts all day, consider reducing the number of doors that are accessible.
- If having dignitaries or VIPs, plan to provide a security detail to ensure their safety.

Off-site Excursions and Events

- If providing a trip to an off-site location, take precautions to ensure you have medical and contact information for each attendee.
- Permission waivers are essential for youth to attend any event off-site.
- Ensure that you have adequate adults to youth ratios.
- Prepare contingency travel advice or plans to include how to get home if your primary method of transport becomes unavailable because of an incident.
- Ensure each member of your group, including children and volunteers, have ID on them in case they are taken ill separated from the group.
- Identify a person who will be a central coordinator in the event of an emergency such as a terrorist attack. This person will remain at home (or not with the travelling party) and coordinate contact and liaison if a major incident occurs. Provide their contact number to parents or next of kin.

Opening, Locking, and Closing Procedures

- If your facility has a motion detector alarm, it will provide much comfort to the staff arriving early in the morning. This ensures that no one has entered the building during the night and is waiting for their arrival.
- Open only the necessary doors and windows.
- Do not have the main sanctuary open during the day. Provide smaller prayer rooms instead.
- Direct cameras toward all entrances and exits.
- Keep a key inventory list.
- Prior to locking the building, conduct a walk through, checking windows and doors.
- Ensure that offices and storage areas are locked at all times.

Property Rights

- If the property is not owned by the religious organization, determine with owner your rights to restrict individuals from the property.
- Develop relationship with local law enforcement and review their requirements for arrest if someone violates a trespassing notice.

- Build relationships with religious leaders in your community.
- Establish a networking group with other religious leaders in your community to share best practices and intelligence information regarding safety and security. Monitor open source intelligence information related to threats against HOWs for criminal, cybercrime, and terrorist activities.
- Include all faiths in your special events.
- In the event of a terrorist attack, we are all one people with one faith.
- Develop an interfaith security council, comprised of facilities/security personnel from HOWs in your geographic region, to meet quarterly to discuss issues of mutual concern.

Additional Resources

Crime Prevention for Houses of Worship, 2nd edition, by Paula L. Ratliff. Published by AISIS International, 2015.
https://www.asisonline.org/ASIS-Store/Products/Pages/Crime-Prevention-for-Houses-of-Worship-2nd-Ed-.aspx

ASIS International—Security for Houses of Worship,
https://www.asisonline.org/Membership/Member-Center/Security-Spotlight/Pages/Security-for-Houses-of-Worship.aspx#HOW11https://www.asisonline.org/Membership/Member-Center/Security-Spotlight/Pages/Security-for-Houses-of-Worship.aspx

FEMA, Center for Faith-Based & Neighborhood Partnerships,
https://www.fema.gov/faith

ASIS INTERNATIONAL
Advancing Security Worldwide®

1625 Prince Street
Alexandria, VA 22314
+1.703.519.6200
asisonline.org