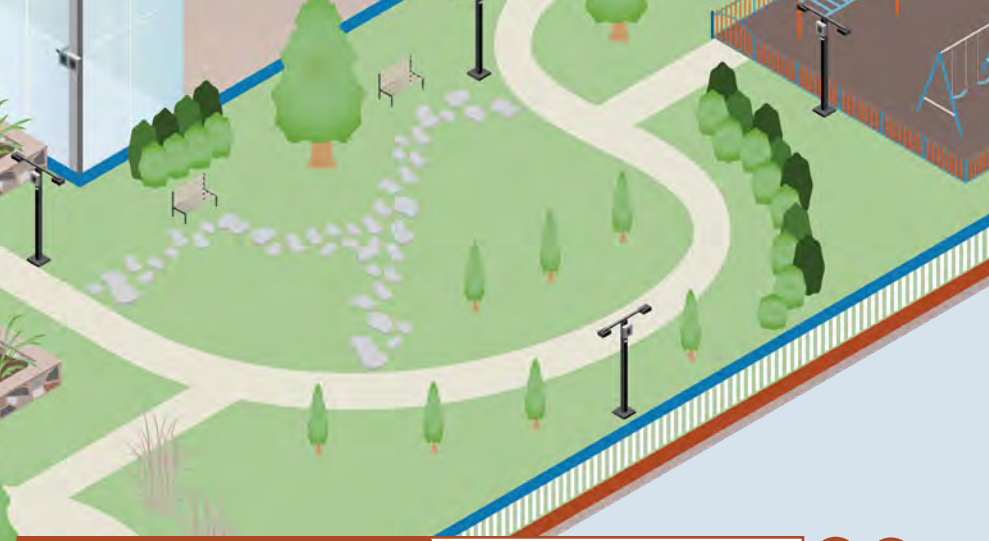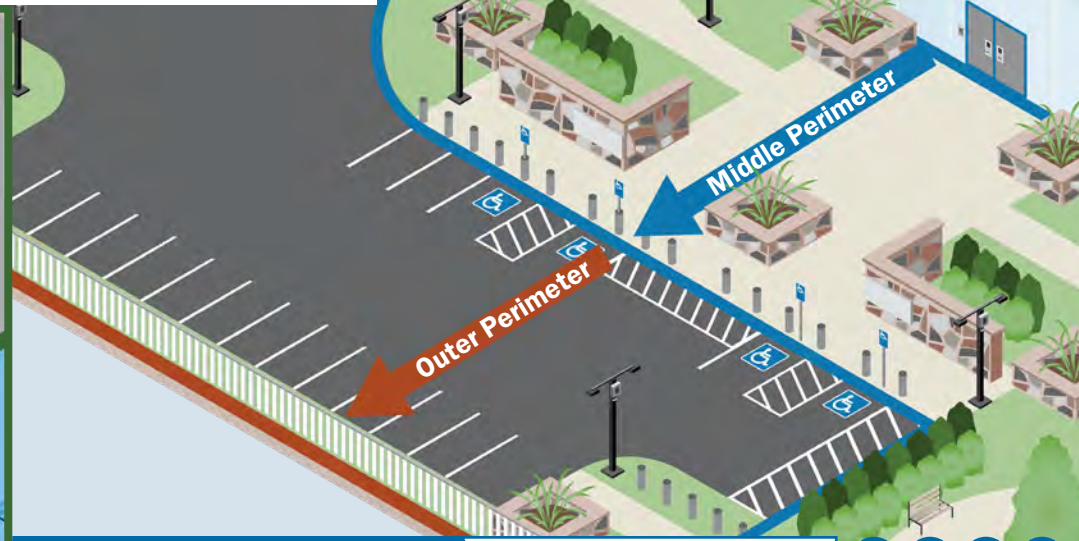# PROTECTING HOUSES OF WORSHIP:
Perimeter Security Considerations

This resource is a companion piece to CISA's and the Federal Bureau of Investigation's (FBI) co-branded Protecting Places of Worship: Six Steps to Enhance Security Fact Sheet, which highlighted the following steps:

1. Understand the Risk
2. Understand Your Space
3. Develop and Practice a Plan
4. Inform and Educate Greeters
5. Pursue Grants
6. Report Hate Crimes and Other Incidents

This infographic outlines low- to no-cost solutions to help implement these suggested practices and highlights ways to identify funding for security improvements. To learn more about layered security and other recommended mitigations, visit CISA's Mitigating Attacks on Houses of Worship Security Guide.

Middle Perimeter

Outer Perimeter

INNER PERIMETER — Corresponds to Six Steps: 1 2 3 4

Area that includes the main building interior and the interiors of any outbuildings.

Access Control: Ensure doors work properly and lock from the inside. Consider limiting entry points and locking doors during events. If financially feasible, implement card swipe access control. Train staff to respond with appropriate measures—ranging from de-escalation to calling 9-1-1, as appropriate—when they observe behaviors of concern.

First Aid/AED: Provide STOP THE BLEED®, CPR, and emergency first aid training for all staff and appropriate members/volunteers. Place life-saving equipment in clearly marked locations and conduct regular inventory/testing. Install fire alarms and smoke detectors, and test them with local first responders annually as part of an Emergency Action Plan (EAP).

Create a Security Team: Establish a working group to create and implement a holistic plan to mitigate risks, train volunteers, and put the congregation's security plan into practice.

Maintain Situational Awareness: Train reception staff and volunteers in identifying suspicious activity or behaviors at the point of entry and/or greeting. Maintain situational awareness of unknown persons or those whose behavior has previously indicated the potential for violence.

Shelter-in-Place Room: Designate optimal shelter-in-place locations (thick/fortified walls, solid doors with locks, minimal interior windows, and first aid emergency kits). Ensure staff and congregants can identify locations through training and signage.

MIDDLE PERIMETER — Corresponds to Six Steps: 2 3 4 6

Fluid area that includes anything on property but outside the main building.

Awareness: Station security team members beyond the building's front doors to maintain situational awareness and identify behaviors of concern while greeting visitors. If possible, perform periodic exterior building sweeps to identify any discrepancies. Train security team members on reporting/notification procedures for rapid law enforcement response.

Doors: Install electronic doorbells to help identify visitors and/or detect intruders before they reach the inner perimeter. Use solid, thick doors to help limit/block access when congregants are inside, along with appropriate locking hardware. Ensure careful key control among current and former members.

Windows: Lock and install alarms on windows, ensuring they can be unlocked for emergency escape. Where feasible, use blast-resistant glass film. Install pull chain or center pull deployable window shades for quick and reliable closing if perceived threat detected.

Emergency Communication: Implement a public notification system that is audible throughout the campus. Provide security team and other key members with handheld radios, and ensure all are familiar with their use. Create threat reporting and response notification procedures, and ensure all congregants are well-versed in how to respond to alerts.

Landscaping: Consider preventive landscaping features, such as large planters, to direct traffic or discourage unauthorized vehicle access. Ensure landscaping does not obscure or obstruct other security measures.

OUTER PERIMETER — Corresponds to Six Steps: 2 4

Area that includes surface parking and outline of primary and outbuildings at the property border, dumpsters, and organization-owned vehicles.

Closed-Circuit Television (CCTV): If financially feasible, consider installing a surveillance system, including cameras offering a clear view of the facility perimeter and individuals approaching the entrance from outside. Consider installing monitor inside lobby and in adminstrative offices. Ensure remote access for select security team members and law enforcement.

Landscape: Remove obscuring brush to increase visibility for staff, congregants, and potential first responders.

Lighting: Consider strategically placing photo-cell (for dusk to dawn) and motion-activated lighting throughout the outer perimeter. Ensure proper maintenance for full functionality.

Traffic Management: Use active and/or passive vehicle barriers. Position proper signage for parking and pathways. Engage trained and properly identified greeters, volunteers, and/or law enforcement to manage traffic. Consider using traffic cones, jersey barriers, and/or other bollards.
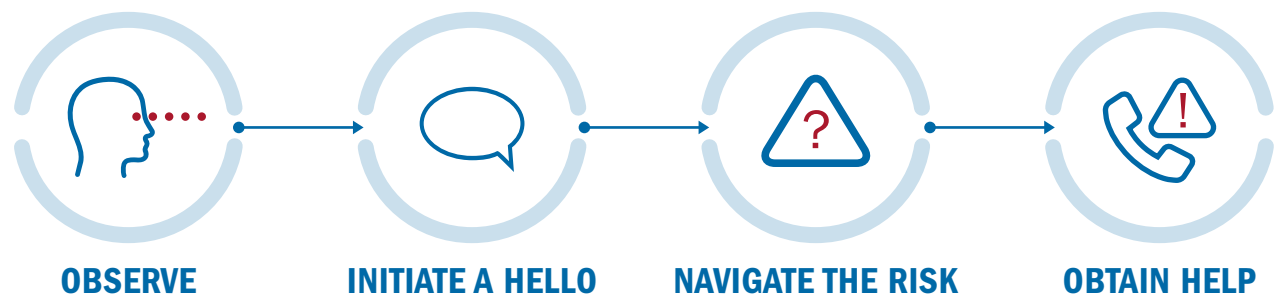
This product describes activities and behaviors that may be suspicious or indicate criminal activity. These activities may be constitutionally protected and should be reported only when there are concrete facts to support a rational conclusion that the behavior is suspicious. Do not report based solely on protected activities, race, religion, gender, sexual orientation, or a combination of such factors.

POWER OF HELLO (1) (2) (3) (4) (6)

Alert employees can spot suspicious activity and report it. The power is in the employee, citizen, patron, or any person who can observe and report. The OHNO approach—Observe, Initiate a Hello, Navigate the Risk, and Obtain Help—helps employees observe and evaluate suspicious behaviors, and empowers them to mitigate potential risk, and obtain help when necessary.

OBSERVE → **INITIATE A HELLO** → **NAVIGATE THE RISK** → **OBTAIN HELP**

ALL PERIMETER LAYERS (1) (2) (3) (4) (6)

Reporting:
Ensure all personnel are empowered to call 9-1-1 in the event of an imminent incident. Visit See Something, Say Something® for more tips on reporting suspicious behavior.

Awareness:
Know your neighbors to share localized threat information. Engage with your local fusion center, Federal Bureau of Investigation (FBI) field office, and local law enforcement to maintain awareness of known threats.

Crime Prevention Through Environmental Design (CPTED):
When considering renovations or new additions, follow CPTED principles to reduce or eliminate vulnerabilities layer by layer. Review the Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks - FEMA 430 (Appendix A) for more information.

⚠ RISK (1) (2) (3) (4) (6)

Facilities face a varying amount of risk due to their unique physical layout and activity footprint. As the facility security team begins to determine vulnerabilities, consider how risk is defined:

Risk = Threat x Vulnerability x Consequence

Risk: The potential for an adverse outcome assessed as a function of hazard/threats, assets and their vulnerabilities, and consequences.

Example: Active shooter (threat) enters facility premises via a broken fence (vulnerability) and attacks staff and congregants, causing loss of life (consequence).

Layered Security Approach:
Frame your facility's security effort through a lens of **outer, middle, and inner perimeters.**

Coordination: Follow a cohesive and thorough security approach, addressing all layers of the perimeter and integrating suspicious behavior security training and skills.

Planning Considerations (3)

Resources to enhance security before an incident and how personnel/volunteers should respond during and following an incident.

Houses of Worship:
cisa.gov/topics/physical-security/protecting-houses-worship

Active Shooter Emergency Action Plan Product Suite:
cisa.gov/resources-tools/resources/active-shooter-emergency-action-plan-product-suite

Active Shooter Preparedness: cisa.gov/topics/physical-security/active-shooter-preparedness

FEMA Guide for Developing Emergency Plans for Houses of Worship:
fema.gov/node/guide-developing-high-quality-emergency-operations-plans-houses-worship

Power of Hello: cisa.gov/topics/physical-security/non-confrontational-techniques/power-hello

De-Escalation Series: cisa.gov/resources-tools/resources/de-escalation-series

Conduct Vulnerability Assessments (1)

Resources to guide personnel at houses of worship through a security-focused self-assessment to understand potential vulnerabilities and identify options for consideration in mitigating those vulnerabilities.

Houses of Worship Security Self-Assessment:
cisa.gov/houses-worship-security-self-assessment

School Security Assessment Tool (SSAT):
cisa.gov/school-security-assessment-tool

Local Resources (1) (2) (3) (4) (5) (6)

CISA Protective Security Advisors (PSAs) are trained subject matter experts who assist with infrastructure protection and vulnerability mitigation.

CISA PSAs: cisa.gov/resources-tools/programs/protective-security-advisor-psa-program

State and Major Urban Area Fusion Centers:
dhs.gov/fusion-centers

FBI-led Joint Terrorism Task Forces:
fbi.gov/investigate/terrorism/joint-terrorism-task-forces

Visit cisa.gov/about/regions or email central@cisa.dhs.gov to contact your local CISA PSA and explore more best practices for house of worship risk assessment and mitigation.

Training and Exercises (3)

Provide annual training for staff and congregants, including children's care personnel and individuals with access and functional needs.

CISA Tabletop Exercise Package (CTEP) for Faith-Based Organizations:
cisa.gov/resources-tools/resources/physical-security-scenarios

STOP THE BLEED®: stopthebleed.org/

Office for Bombing Prevention (OBP) Training Program: cisa.gov/resources-tools/programs/office-bombing-prevention-obp-training-program

Grant Information (5)

Grants can be used by state, local, tribal, and territorial jurisdictions for training, exercises, planning, personnel, and equipment to prepare for many threats and hazards.

DHS Grants: dhs.gov/dhs-grants

Nonprofit Security Grant Program:
fema.gov/grants/preparedness/nonprofit-security

School Safety Grants Finder Tool:
schoolsafety.gov/grants-finder-tool

Targeted Violence and Terrorism Prevention Grant Program: dhs.gov/tvtgrants

To access the digital version of this guidance, follow the QR code below: