Physical Security Performance Goals for Faith-Based Communities

DECEMBER 2023

PERFORMANCE GOALS

Version 1.0

A LETTER FROM OUR DIRECTOR

As the National Coordinator for critical infrastructure security and resilience, the Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure Americans rely on every day.

As noted in the 2024 Homeland Threat Assessment issued by the U.S. Department of Homeland Security (DHS), the threat of violence from individuals radicalized in the United States will "remain high . . . marked by lone offenders or small group attacks that occur with little warning." In this dynamic threat environment, ideological differences can result in attacks anywhere, including at houses of worship. This fact is made evident by the persistent threats and senseless attacks occurring at churches, synagogues, temples, mosques, and other faith-based locations. The goal of these attacks is to weaken the fabric of our nation; together, we must do everything possible to protect our citizens, our infrastructure, and our way of life. To address this rising concern in partnership with faith-based leaders, DHS Secretary Alejandro Mayorkas reconstituted the Faith-Based Security Advisory Council to provide recommendations on matters related to protecting houses of worship and to enhance coordination with the faith community.

CISA remains fully committed to its longstanding partnership with faith-based leaders to advance the protection of houses of worship while preserving their open and welcoming environments. Through a multitude of capabilities, the agency supports faith-based communities in improving physical and cyber security practices. To that end, CISA developed this guide in partnership with multiple leaders and security experts from interfaith groups and several other DHS programs to introduce foundational benchmarks for implementing simple cost-effective measures to bolster security.

I encourage you to use this guide to establish or improve security practices that keep your house of worship and congregants safe and secure. Thank you for your continued dedication to maintaining a partnership with CISA to collaboratively protect our communities.

JEN

Jen Easterly
Director, Cybersecurity and Infrastructure Security Agency

December 2023

BACKGROUND AND CONTEXT

The Physical Security Performance Goals for Faith-Based Communities—the first in a series of impending related documents geared toward industry partners—are a set of physical security practices that houses of worship and related facilities can use to reduce security risks to their congregations.

Faith plays an important role in communities across the United States, from providing social services such as food, shelter, and clothing, to fostering a sense of unity for those with similar spiritual beliefs. These welcoming communities are often physically centered around houses of worship, which strive for the right balance between security and accessibility.

The Cybersecurity and Infrastructure Security Agency (CISA) is committed to partnering with faith groups to help mitigate the threat of targeted violence and prepare for potential incidents. To support communities, CISA developed these performance goals to provide readily implementable, cost-effective solutions that can reduce risk.

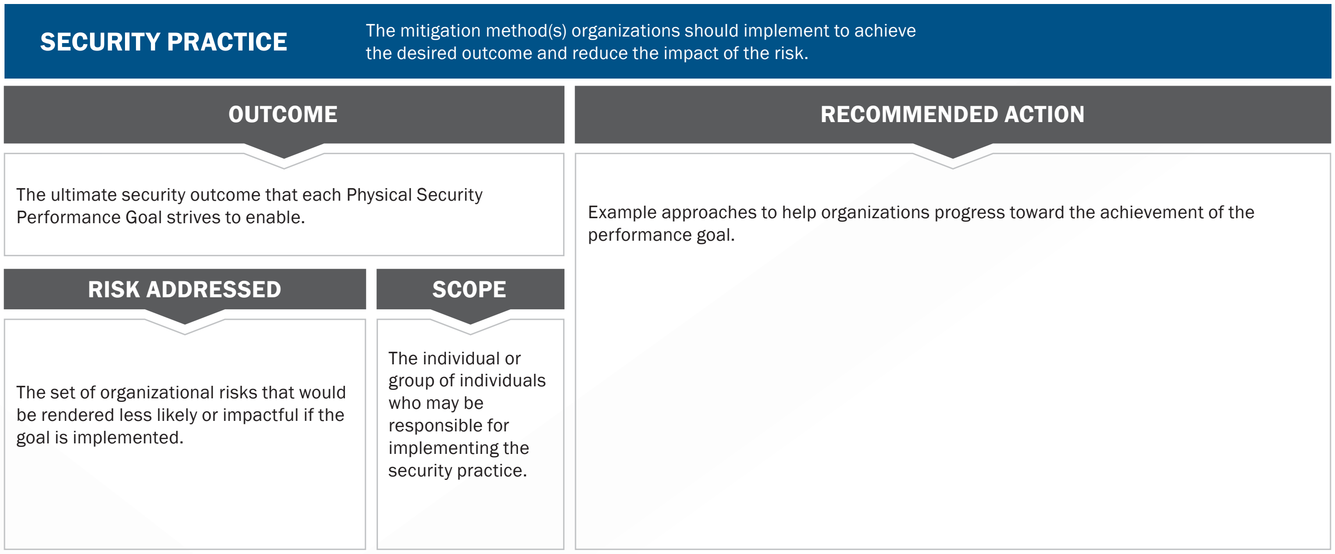
Once developed and broadly applied, the performance goals will enable houses of worship and related facilities—particularly those with limited resources—to effectively identify and manage risk.

THE MODEL

The Physical Security Performance Goals model provides recommended considerations aligned with security best practices to mitigate identified threats. The model examines threats and vulnerabilities to provide targeted mitigation strategies, all of which are organized by the following functional categories: **Identify, Protect, Detect, Respond,** and **Recover.** This framework directly complements the five mission areas of the National Preparedness Goals, which are to prevent, protect against, mitigate, respond to, and recover from threats and hazards that pose the greatest risk.

The security performance goals in this document are displayed in a visual model to help readers understand not only the goals themselves, but also the intended outcomes, risks that the security goals address, and a benchmark for robust security practices. For additional information and context, please see the Resources section located at the end of the document. For best practices related to cybersecurity, please see the Cross-Sector Cybersecurity Performance Goals.

Each goal is comprised of the following components:



SECURITY PRACTICE The mitigation method(s) organizations should implement to achieve the desired outcome and reduce the impact of the risk.

OUTCOME

The ultimate security outcome that each Physical Security Performance Goal strives to enable.

RISK ADDRESSED

The set of organizational risks that would be rendered less likely or impactful if the goal is implemented.

SCOPE

The individual or group of individuals who may be responsible for implementing the security practice.

RECOMMENDED ACTION

Example approaches to help organizations progress toward the achievement of the performance goal.

The Physical Security Performance Goals for Faith-Based Communities are intended to:

- Establish a baseline set of physical security practices broadly applicable across houses of worship and related facilities with known risk factors.
- Create benchmarks to measure and improve physical security maturity and build community readiness and resilience.
- Articulate actionable guidance, including a prioritized set of physical security practices.
- Provide a unique tool to identify security gaps and create an actionable plan that aligns with the priorities of faith-based communities.

The Physical Security Performance Goals for Faith-Based Communities are:

- **Voluntary:** These physical security goals are offered as options to enhance security posture and risk tolerance but do not place any obligation on a house of worship. This information can and should be tailored to the needs of each individual facility.
- **Not Comprehensive:** These physical security goals do not identify all the physical security practices needed to protect houses of worship. The goals capture a core set of practices with known security approaches that are broadly applicable. Considerations for implementation should include the size of the organization and unique challenges specific to the institution and its community. Baselines should be tailored to the needs of individual houses of worship.

GETTING STARTED

For houses of worship to successfully implement the security goals, consider identifying a security coordinator and additional security and safety planning team members (if possible) to develop a holistic security strategy. To effectively manage risk, ensure that:

- Risk assessments are conducted to understand the organization's exposure to risk.
- Facilities, people, activities, and processes are identified.
- Relevant hazards, threats, and consequences to the organization are identified and documented.
- Evaluations on the likelihood of occurrence and effectiveness of existing controls are conducted.
- Mitigation strategies are developed, implemented, and regularly re-evaluated to ensure continuous improvement and adaptability.

Organizations are also encouraged to leverage CISA Protective Security Advisors (PSAs)—security subject matter experts located across the country who directly support faith-based communities with vulnerability assessments, site visits, and training at no cost.

CONTENTS

IDENTIFY

1.A FORM A SECURITY AND SAFETY PLANNING TEAM

OUTCOME

An established group of staff and volunteers focused on maintaining the safety and security of the house of worship and related facilities.

RISK ADDRESSED

Uncoordinated and ad hoc approach to security, potentially increasing vulnerabilities.

SCOPE

Faith-based leaders

Staff

Volunteers

RECOMMENDED ACTION

- Identify a lead who will serve as the primary decision maker for security-related matters. Ideally, this will be a staff member or engaged volunteer with relevant professional experience.
- Form a team of staff and volunteers composed of varying individuals representative of the community who can collaboratively evaluate security requirements and generate recommendations for improvements.
- Screen prospective team members with basic background checks and a brief interview; establish a standard waiting period before assigning volunteers to serve in key capacities to provide sufficient time to get to know individuals.

1.B IDENTIFY RISK

OUTCOME

Increased awareness and understanding of potential risks, inclusive of threats, vulnerabilities, and consequence factors.

RISK ADDRESSED

Lack of awareness of potential risks to houses of worship, precluding accurate security-based decision making.

SCOPE

Faith-based leaders

Staff

Volunteers

RECOMMENDED ACTION

- Review national threat information, such as the U.S. Department of Homeland Security (DHS) Homeland Threat Assessments, to understand the evolving national threat landscape.
- Reference information regarding more imminent threats through the DHS National Terrorism Advisory System Bulletins.
- Establish relationships with State Fusion Centers to gain access to relevant regional/state threat information.
- Connect with local law enforcement agencies or Federal Bureau of Investigation (FBI) field offices to better understand the local perspective and threat actors. Take advantage of opportunities and listservs with relevant security topics and access security resources as they are released.
- Establish a mutually supportive relationship with the local community and faith-based organizations to exchange threat-related information.
- Conduct a risk assessment, either supported or through self-assessment tools, to inform planning considerations, mitigation strategies, and funding/investment requirements.
- Prioritize assessed risks to assist with determining future protective investments, including no- to low-cost improvements.

1.C CREATE SECURITY, RESPONSE, AND RECOVERY PLANS

OUTCOME

Documented procedures to enhance security and mitigate the impacts of an incident to the house of worship and congregants.

RISK ADDRESSED

Inability to reduce the impacts of an attack and increased difficulty in recovery.

SCOPE

- Faith-based leaders
- Staff
- Volunteers
- Security and safety planning team

RECOMMENDED ACTION

- Create a security plan outlining key steps staff and volunteers should take to improve security.
- Develop threat-specific emergency operations plans that delineate processes and procedures that the house of worship and related facilities will take when responding to and recovering from an incident.

PROTECT

2.A INCORPORATE SECURITY MEASURES

OUTCOME

Improved security through the implementation of tangible security protocols.

RISK ADDRESSED

Lack of established security protocols.

SCOPE

- Faith-based leaders
- Staff
- Volunteers

RECOMMENDED ACTION

- Implement improvements or incorporate additional measures to address the security gaps identified as areas of concern from risk assessments.
- Monitor parking areas and all access and entry points with video surveillance systems.
- Place photocell (for dusk to dawn) and motion-activated LED lighting throughout the exterior perimeter.
- Lock and install alarms on windows and doors, ensuring they can be unlocked for emergency escape.
- Ensure doors work properly and lock from the inside. Do not prop doors open.
- Use signage and other communication methods to indicate unauthorized areas.
- Keep landscaping trimmed. Avoid tree branches below six feet and prevent bushes from growing above two feet to prevent hiding places.
- Ensure fences and gates are maintained and in working order.
- Incorporate access control for critical areas such as IT/electrical rooms, finance offices, and children's ministries.
- Train appropriate personnel in active threat response and shelter-in-place procedures.
- For schools and daycares on property:
    - Limit access to as few people as possible using a single point of entry, secure other access points, and ensure only authorized visitors are allowed entry with photo identification. Consider using a visitor management system.
    - Establish communication procedure with parents or guardians of minors in the event of an ongoing incident.

2.B IMPLEMENT CYBER HYGIENE

OUTCOME

Identities and data are protected from cyber threats.

RISK ADDRESSED

Insufficient foundational cybersecurity practices that result in risks to systems and networks.

SCOPE

- Faith-based leaders
- Staff
- Volunteers

RECOMMENDED ACTION

- Update software/hardware on regular basis.
- Require strong passwords for access.
- Secure all data and files on the network, and secure router with encryption methods.
- Periodically check for unauthorized connections or devices.

2.C ESTABLISH PARTNERSHIP WITH LAW ENFORCEMENT AND KEY COMMUNITY RESOURCES

OUTCOME

Coordinated security and response protocols.

RISK ADDRESSED

Delayed or lack of support during an incident.

SCOPE

- Faith-based leaders
- Staff
- Volunteers
- Local law enforcement and first responders
- Leaders of neighboring houses of worship

RECOMMENDED ACTION

- Build a strong relationship with law enforcement to help them understand any unique community customs or requirements. Share facility floor plans.
- Build relationships with neighboring houses of worship and counseling resources to create options for information sharing and response activities, such as family assistance centers.
- Offer facility to support training opportunities for first responders.

2.D UTILIZE PERSONAL SECURITY BEST PRACTICES

OUTCOME

Enhanced personal and online security.

RISK ADDRESSED

Personal behaviors that can increase security risks.

SCOPE

- Faith-based leaders
- Staff

RECOMMENDED ACTION

- Protect personal residences by installing or improving security systems, securing all entry points and the perimeter of the home, and maintaining outdoor property structures like walls and fences.
- Remain aware of surroundings and exercise caution with potential visitors.
- Use varying routes when commuting.
- Exercise caution online by:
  - Installing apps only from reputable sources.
  - Monitoring emails for suspicious content.
  - Ensuring devices are up to date.
  - Utilizing third-party vendors to scrub online presence.
- Be careful when posting any location information online, as it can be used in doxing—the practice of using personal information for malicious purposes.
- Limit information provided during live streams and other events to only what needs to be conveyed.

2.E CONDUCT TRAINING AND EXERCISES

OUTCOME

Trained, capable people and increased capacity of personnel to support incident response in order to mitigate the impacts of an incident.

RISK ADDRESSED

Uncoordinated or ad-hoc security that precludes the identification of potential risk and the ability to effectively act following an incident.

SCOPE

- Faith-based leaders
- Staff
- Volunteers
- Local law enforcement and first responders
- Students

RECOMMENDED ACTION

- Train staff and volunteers on specific threats (active shooter, bombing, vehicle ramming) on a regular basis to increase awareness of best practices.
- Collaborate with law enforcement and emergency responders to conduct exercises to enhance response capabilities.
- Conduct after-action reviews to identify any lessons learned and areas for improvement; document findings in an improvement plan.
- For schools and daycares on property:
  - Conduct drills for students and staff to test the processes, procedures, and technologies of the school facility.

2.F PRIORITIZE FUNDING FOR SECURITY

OUTCOME

Increased availability of funding to incorporate additional security measures.

RISK ADDRESSED

Limited budget for security that results in unaddressed vulnerabilities.

SCOPE

- Faith-based leaders

RECOMMENDED ACTION

- Identify internal funding mechanisms and, where appropriate, solicit funding from congregants.
- Pursue grant opportunities provided by DHS and the Department of Justice that focus on physical security enhancements and those that support the establishment and enhancement of local prevention efforts.
- Contact non-profit organizations that provide security resources to assist with community-specific needs.

3 IDENTIFY SUSPICIOUS ACTIVITY AND DETERMINE POTENTIAL SUSPICIOUS BEHAVIORS

OUTCOME

Early detection of suspicious activity that prevents or mitigates a potential threat.

RISK ADDRESSED

Inability of staff and volunteers to recognize suspicious behaviors or determine a potential threat.

SCOPE

- Faith-based leaders
- Staff
- Volunteers
- Congregants

RECOMMENDED ACTION

- Provide situational awareness training to help individuals quickly identify potential threats/hazards to allow for appropriate response to an incident.
- Utilize greeters at every entry point and parking lot to identify early warning signs of potential violence.
- For schools and daycares on property:
  - Create a culture of reporting concerning behaviors. Students and staff may report concerns through a variety of ways (online forms, phone number, email, or application platforms).
  - Establish a team that will assess a student's behavior and provide intervention strategies such as counseling, mental health care, or social and family services.

RESPOND

4.A IMPLEMENT RESPONSE PLAN

OUTCOME

Comprehensive response plans are executed immediately after an incident to minimize damage and save lives.

RISK ADDRESSED

Increased facility damage and casualties due to delayed response.

SCOPE

- Faith-based leaders
- Staff
- Volunteers
- Local law enforcement and first responders

RECOMMENDED ACTION

- Implement response plan immediately to address preservation of life, incident stability, and property preservation.
- Dial 9-1-1.
- Implement an emergency communication process that provides internal and external notifications.
- For schools and daycares on property:
    - Alert students, staff, law enforcement, and parents of the emergency. Notifications can come from alarms, announcements, mass text messages, phone applications, emails, or other forms.

4.B ESTABLISH A REUNIFICATION LOCATION

OUTCOME

Implementation of reunification plan and utilization of previously identified reunification sites.

RISK ADDRESSED

Inability to safely reunite victims/families and provide support services.

SCOPE

- Faith-based leaders
- Staff
- Volunteers
- Leaders of neighboring houses of worship

RECOMMENDED ACTION

- Establish a reunification and/or family assistance center immediately following an incident.
- Develop a plan for mental health management in the event of a major incident.
- For schools and daycares on property:
    - Communicate the reunification area to parents/guardians.

RECOVER

5.A RECONSTITUTE SERVICES AND PROVIDE MEMORIALIZATION

OUTCOME

Safe environment is re-established and services resume.

RISK ADDRESSED

Further psychological and emotional impacts due to prolonged closure of the house of worship or related facility.

SCOPE

Faith-based leaders

Staff

Volunteers

RECOMMENDED ACTION

- Execute the recovery plan.
- Assess damages, secure funding resources, contact insurance, contact appropriate remediation services needed to resume operations, and establish mental health support.
- Ensure there is a dedicated location for the community to reflect and memorialize those impacted by the incident; take care to respectfully bring down memorials. Establish a means for appropriate storage of gifts and proper accounting of donations of money.
- Allow law enforcement to document and recover evidence to conduct a complete investigation.

5.B DEVELOP AFTER-ACTION REVIEW

OUTCOME

Review of incident response and identification of areas for improvement/corrective action to improve security measures.

RISK ADDRESSED

Lack of awareness regarding potential areas for improvement, leading to sustained vulnerabilities.

SCOPE

Faith-based leaders

Staff

Volunteers

RECOMMENDED ACTION

- Develop an after-action review that addresses deficiencies to reduce damage/ casualties in the future.
- List areas for improvement/corrective action to address gaps in response plan.
- Share after-action review with trusted neighboring houses of worship to assist them in better addressing security gaps.

5.C IMPLEMENT RECOMMENDATIONS IDENTIFIED IN AFTER-ACTION REVIEW

OUTCOME

Findings of after-action review address gaps resulting in improved safety and security.

RISK ADDRESSED

Repeating actions that have been identified as inefficient response procedures.

SCOPE

Faith-based leaders

Staff

Volunteers

RECOMMENDED ACTION

- Implement further security measures that address vulnerabilities identified in after-action review.

GLOSSARY

Access Point: Physical entry points.

Active Assailant: One or more individuals actively engaged in killing or attempting to kill people in a populated area.

After-Action Review: Developed after an incident or exercise to document strengths to be maintained and built upon, and to identify potential areas for improvement.

Consequence: The effect of an event, incident, or occurrence.

Cyber Hygiene: Maintaining basic levels of cybersecurity and improving general awareness to enhance resilience and mitigate the effects of a potential intrusion or attack.

Doxing: Internet-based practice of gathering an individual's personally identifiable information—or an organization's sensitive information—from open source or compromised material and publishing it online for malicious purposes.

Entry Point: The location where individuals may enter a facility; see access point.

Family Assistance Center: Area or location to provide services for evacuees and their families; can also assist with reunifications for survivors with family or friends.

Fusion Center: State-owned and operated centers that serve as focal points in states and major urban areas for the receipt, analysis, gathering, and sharing of threat-related information between all levels of government and private sector partners.

Grant: A sum of money given by a government or other organization for a particular purpose; the principal funding mechanism to commit and award federal funding to eligible state, local, tribal, territorial, certain private non-profits, individuals, and institutions of higher learning.

Incident: An assessed occurrence having potential or actual adverse effects on the organization. A security incident is an incident or series of incidents that violate the security policy. Any event affecting the safety, security, or protection of a property, facility, or occupant that requires response, investigation, or other follow up.

Information Sharing: The passing or exchange of information between people or entities.

Mitigation: Actions taken to reduce loss of life and property by lessening the impact of disasters, including but not limited to community-wide risk reduction projects; efforts to improve the resilience of critical infrastructure and key resource lifelines; risk reduction for specific vulnerabilities from natural hazards or acts of terrorism; and initiatives to reduce future risks after a disaster has occurred.

Network: A group of two or more computers or other electronic devices that are interconnected for the purpose of exchanging data, sharing resources, or storing information.

Personal Security: Actions taken to mitigate or reduce the probability of becoming a victim of an attack.

Physical Security: Protection from threats that could cause losses or damages. Maintaining a strong physical security posture is an ongoing process that involves a continual assessment of new assets and changing threats.

Protective Security Advisor (PSA): Security subject matter experts located across the country who directly support the critical infrastructure community in enhancing security.

Recovery: The return to normal business operations following an incident, crisis, disaster, or significant event.

Recovery Plan: The policies and procedures that position organizations to effectively recover from an active assailant, weather event, or other incident, while providing the best support structure for their employees, contractors, visitors, patrons, family members, and the community at large.

Response: Focuses on the immediate and short-term effects of an event/incident/disaster. It is usually focused on preservation of life and preventing immediate damage.

Response Plan: The deliberate policies and rehearsed procedures that position organizations and the individuals within them to optimally react to an imminent threat.

Reunification: The process of restoring incident evacuees and survivors with their family and friends.

Reunification Plan: A written document that sets forth the steps to be taken to restore evacuees and survivors with their family and friends.

Risk: A measure of potential harm from an undesirable event that encompasses threat, vulnerability, and consequence. Potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences; potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident, event, or occurrence.

Risk Assessment: The process of identifying, analyzing, assessing, and communicating risk, and accepting, avoiding, transferring, or controlling it to an acceptable level considering the associated costs and benefits of any actions taken.

Screening: Physical and/or information-based examination or review of cargo, people, and their belongings.

Security Coordinator: The leader of the security and safety planning team responsible for security-related questions.

Security Plan: Strategy with specific courses of action to protect people and key assets from harm during a threatening or hazardous incident.

Security and Safety Planning Team: Supports the Security Coordinator by conducting research, evaluating needs, providing recommendations, and assisting with plan development.

Security Protocol: The overall security strategy or a specific practice or specified procedure within the security plan. Also known as *Security Practice*.

Security Strategy: The established goals, objectives, and courses of actions that make up the protection plan for an organization, its members, and its assets.

Shelter in Place: Response that involves the immediate, orderly moving of site occupants to locations within the facility (indoors or outdoors) that offer relative protection from the natural, technological, or human-caused event; the type of incident/hazard will determine the type of shelter that offers the best protection.

Threat: Natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.

Vulnerability: A physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard; characteristic of design, location, security posture, operation, or any combination thereof, that renders an asset, system, network, or entity susceptible to disruption, destruction, or exploitation.

RESOURCES

IDENTIFY

Security Planning Workbook – assists with developing a foundational security plan.

House of Worship Self-Assessment Tool – enhances understanding of potential vulnerabilities and recommends corresponding risk mitigation solutions.

School Security Self-Assessment Tool – informs schools' safety and security planning process by assessing existing security measures and areas for improvement.

Homeland Threat Assessments – annual overview of the most direct and pressing threats to the United States.

National Terrorism Advisory System Bulletins – provides information about heightened risk of terrorist attacks in the United States and actions that may be taken.

State Fusion Centers – provides information sharing and analysis services.

FBI Field Offices – contact information for 56 field offices located across the country.

Bomb Threats – information to develop a plan, assess, and respond to bomb threats.

PROTECT

Protecting Houses of Worship – website that provides a single entry to a multitude of resources geared toward faith-based communities, including those focused on active shooter, bombing prevention, and other threat-specific information.

Security Advisors – cadre of physical and cyber security experts who can assist in identifying potential vulnerabilities and strategizing security enhancements.

School Safety – provides schools with actionable recommendations to create safe and supportive learning environments for students and educators.

Personal Security Considerations – encourages vigilance and reporting of suspicious behavior to thwart an attack.

Cross-Sector Cybersecurity Performance Goals – provides a select list of attestable goals to reduce cyberthreat to an organization.

Targeted Violence and Terrorism Prevention Grant – provides funding to establish or enhance capabilities to prevent targeted violence and terrorism.

Nonprofit Security Grant – provides funding for physical security enhancements to nonprofit organizations that are at high risk of terrorist attack.

Homeland Security Grant – suite of risk-based grants to assist in preventing, protecting against, mitigating, responding to, and recovering from acts of terrorism and other threats.

CISA Tabletop Exercise Packages – comprehensive set of resources designed to assist organizations in conducting independent exercises using a variety of physical and cybersecurity scenarios, including those specific to faith-based communities.

Improvised Explosive Device (IED) Protective Measures – best practices to identify risks and vulnerabilities to mitigate the IED threat.

DETECT

Power of Hello Houses of Worship Guide – introduces the OHNO Approach: Observe, Initiate a Hello, Navigate the Risk, and Obtain Help to assist staff, volunteers, and visitors in observing and evaluating suspicious behaviors, and obtaining help when necessary.

De-Escalation Series – contains four products to assist personnel to identify and navigate suspicious activity or potentially escalating situations, and to safely disengage and report to local law enforcement or other appropriate authorities.

Making Prevention a Reality – practical guide on assessing and managing the threat of targeted violence with concrete strategies to help communities prevent these types of incidents.

Suspicious Activity and Items – information to recognize unusual behaviors and suspicious items associated with IED threats.

RESPOND

Options for Consideration (Active Shooter Preparedness) Video – demonstrates possible actions that individuals can take if confronted with an active shooter scenario; also shows how to assist authorities once law enforcement arrives.

Public Information Officer (PIO) Program – designed to provide essential knowledge, skills, and abilities to support proper decision-making by delivering the right message, to the right people, at the right time.

IS-907: Active Shooter: What You Can Do – informs of actions to take when confronted with an active shooter and responding law enforcement; recognize potential workplace violence indicators; prevent and prepare for active shooter incidents; and manage the consequences of an active shooter incident.

Bomb Threat Checklist – helps respond to a bomb threat in a controlled manner with the first responders and other stakeholders.

RECOVER

Active Shooter Recovery Guide – assists in the proactive implementation of procedures that best positions the house of worship to most recover from an active shooter incident, while providing the best support structure for their staff, volunteers, and congregants.

Continuity Resource Toolkit – provides tools, templates, and resources to help and maintain a successful continuity plan.