TAMPA POLICE Department

HOUSE OF WORSHIP SECURITY TRAINING

TAMPA S.A.F.E.

*S.A.F.E. = **S**ECURITY **A**WARENESS **F**OR **E**VERYONE*

- **TAMPA SAFE IS A PARTNERSHIP PROGRAM BETWEEN TPD AND COMMUNITY ORGANIZATIONS, DEDICATED TO ENHANCING SAFETY AND SECURITY THROUGH PROACTIVE STRATEGIES.**

- **OUR OBJECTIVE IS TO EMPOWER LEADERS OF HOUSES OF WORSHIP WITH PRACTICAL KNOWLEDGE AND TOOLS TO PROTECT YOUR CONGREGANTS AND PROPERTY.**

AGENDA

- Brief overview of security considerations
- Resources that can be tailored for you
- Question & Answer Session w/ SME’s

RELIGIOUS ESTABLISHMENTS AS TARGETS

- General criminal activity vs targeted attacks

- Religious establishments are often targets of violence and/or criminal activity:

  <u>Logistical Targets</u>

  - Gatherings of large groups in confined environments = target of opportunity

  <u>Ideological Targets</u>

  - Religious establishments may be targeted for beliefs, shock value, political/cultural statements, etc.

THREATS

<u>Internal</u>

- Disgruntled members, employees, etc.
- Offender with ties to a member/leader/associate/etc.—i.e., domestic violence related attack

<u>External</u>

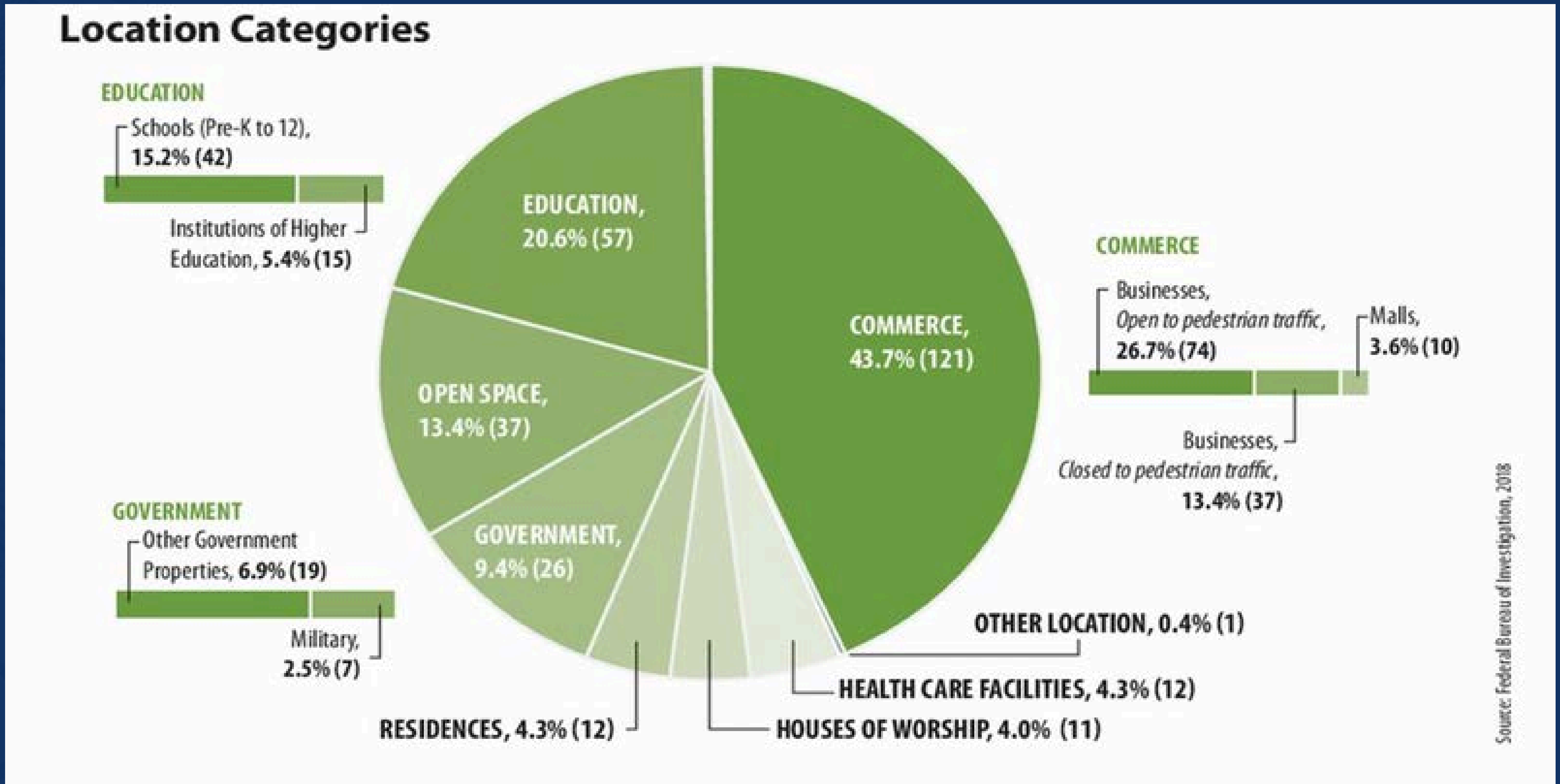
- Offender unrelated to location
- Attacks location based on convenience (lots of people in one place) or for general ideological reasons

TARGETS FOR MASS ATTACKS

- For serious, mass attacks (i.e. “Active Shooters”), houses of worship represent a relatively small percentage of incident locations

- HOWEVER, recent events have continued to highlight that they CAN be a target and the need for preparation

- Other, lesser (but still serious) offenses can still occur with greater frequency



Source: Federal Bureau of Investigation, 2018

FUNDAMENTALS OF SECURITY

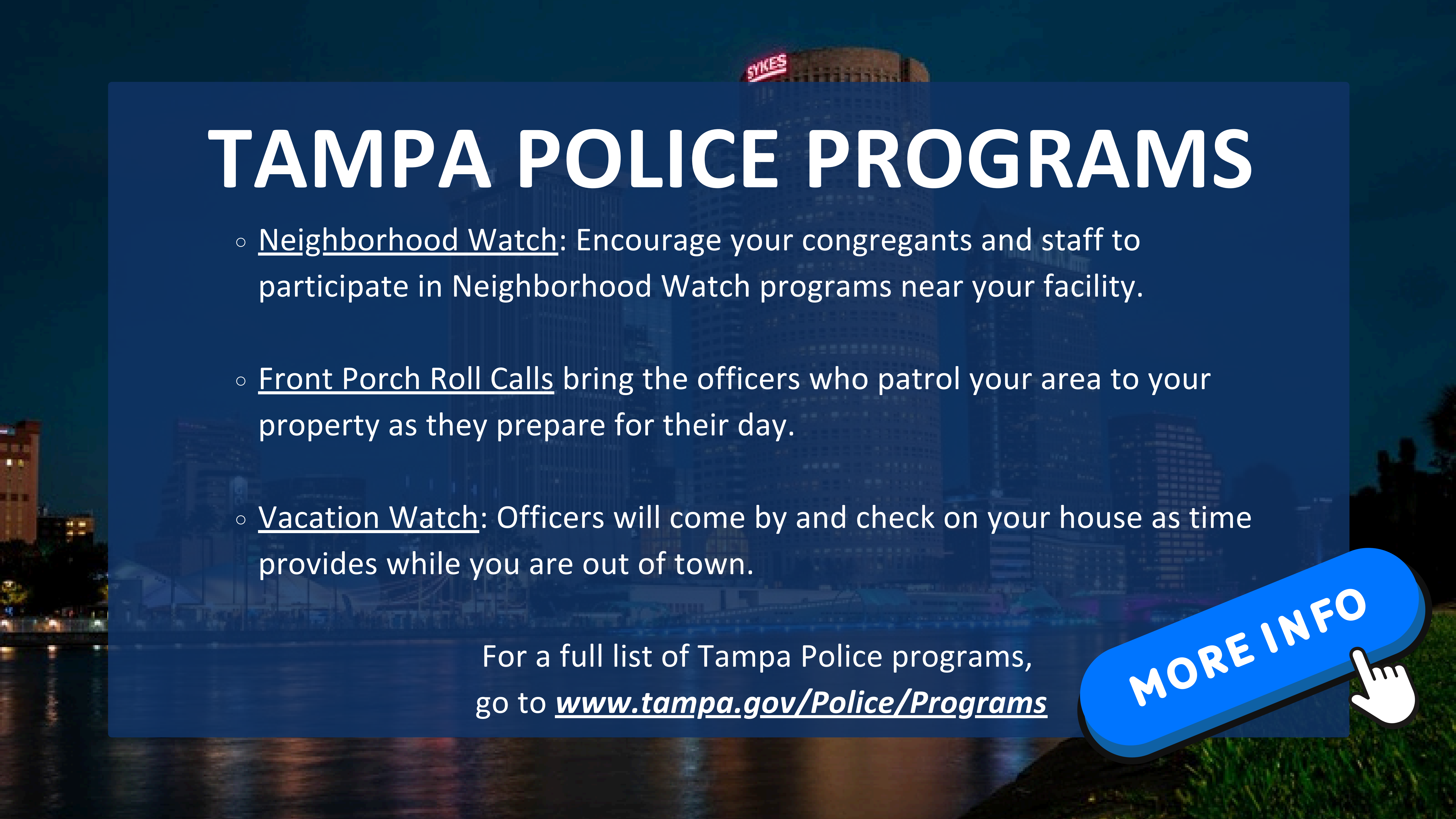
THE FOUR "D's"

- Deter
  - Detect
    - Delay
      - Defend

THE SIX STEPS TO SECURITY

1. UNDERSTAND THE RISKS

- Realistically evaluate your location & establishment (checklists in resources)
- Stay in touch with the Tampa Police Department, or your local agency, for latest updates on criminal activity & threats



TAMPA POLICE PROGRAMS

- Neighborhood Watch: Encourage your congregants and staff to participate in Neighborhood Watch programs near your facility.
- Front Porch Roll Calls bring the officers who patrol your area to your property as they prepare for their day.
- Vacation Watch: Officers will come by and check on your house as time provides while you are out of town.

For a full list of Tampa Police programs,
go to ***www.tampa.gov/Police/Programs***

MORE INFO

SUBSCRIBE

STAY CONNECTED

SUBSCRIBE

www.tampa.gov/TampaPDNews

Subscribe to receive news releases directly to your email.

www.tampa.gov/Police/CommunityNews

Subscribe to keep updated on community events & initiatives.

www.tampa.gov/Police/PALPulse

Keep up with the athletics & activities at the Tampa Police Athletic League!

COMMUNITY ENGAGEMENT BUREAU

General Office Line: **813-276-7011**

E-MAIL US

TPD-CommunityEngagement@tampa.gov

2. UNDERSTAND YOUR SPACE

- Evaluate your facility through a layered approach
- Establish inner, middle and outer perimeters

UNDERSTANDING CPTED: CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN

ACTIONABLE SECURITY IMPROVEMENT CHECKLIST

Lighting & Landscaping

- Lighting: Install or upgrade motion-sensor lighting at vulnerable areas (rear entrance, secluded sides).
- Ensure adequate illumination for all pathways and parking lots.
- Landscaping: Trim bushes below windowsills and prune tree canopies to 6+ feet above the ground to eliminate hiding spots and improve visibility.

Doors & Windows

- Upgrade deadbolt locks to a high-quality, 2-inch throw on critical doors.
- Ensure functioning locks on all accessible windows.
- Implement a key control policy for all access points to track and manage who has keys.

Technology & Protocols

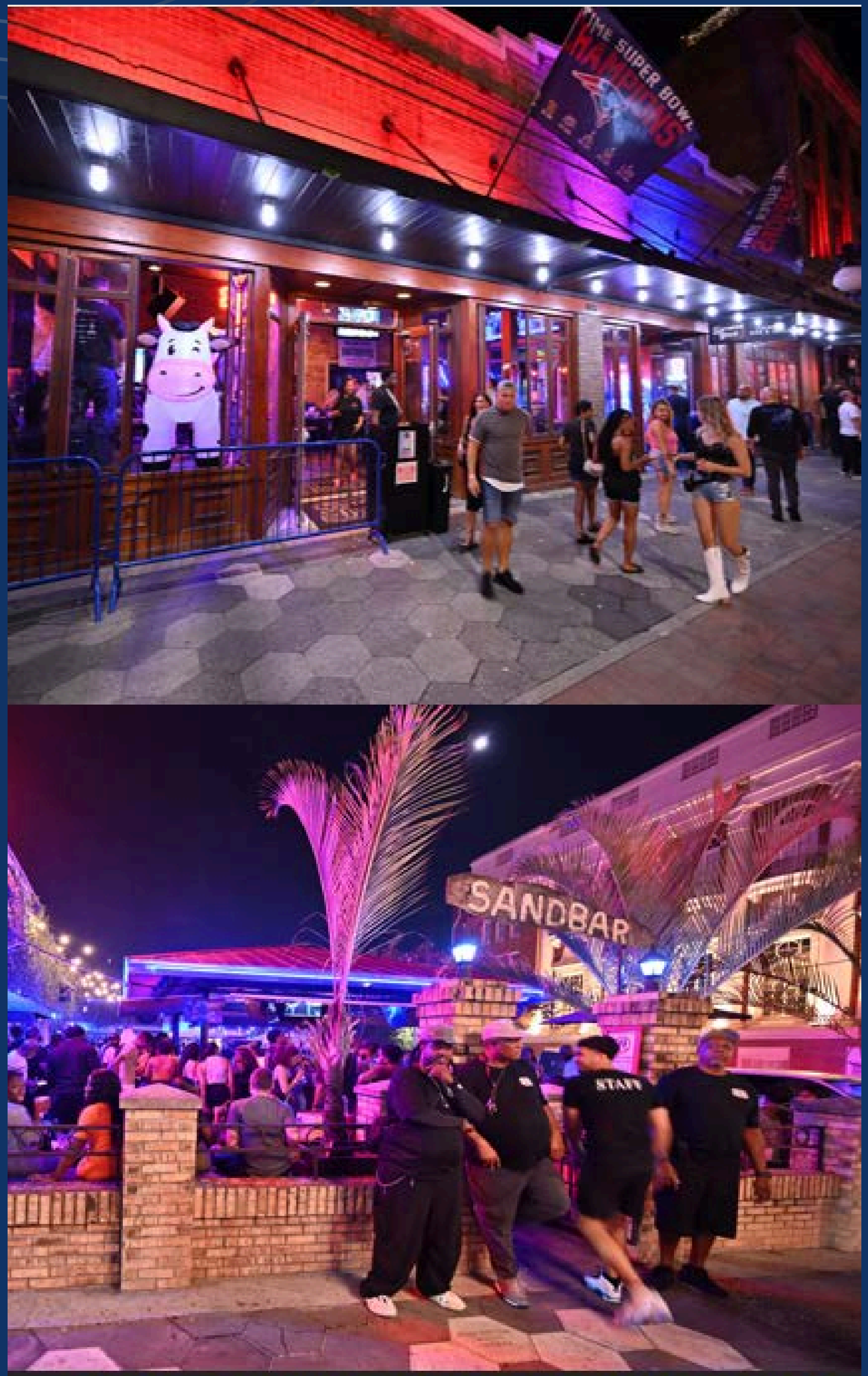
- Consider a monitored alarm system for all access points.
- Evaluate security camera placement for optimal coverage of entry points and high-value areas.
- Develop and regularly review emergency response plans (active threat, fire, medical).
- Conduct regular security training for staff and volunteers.

NATURAL ACCESS CONTROL
(Guiding Movement)

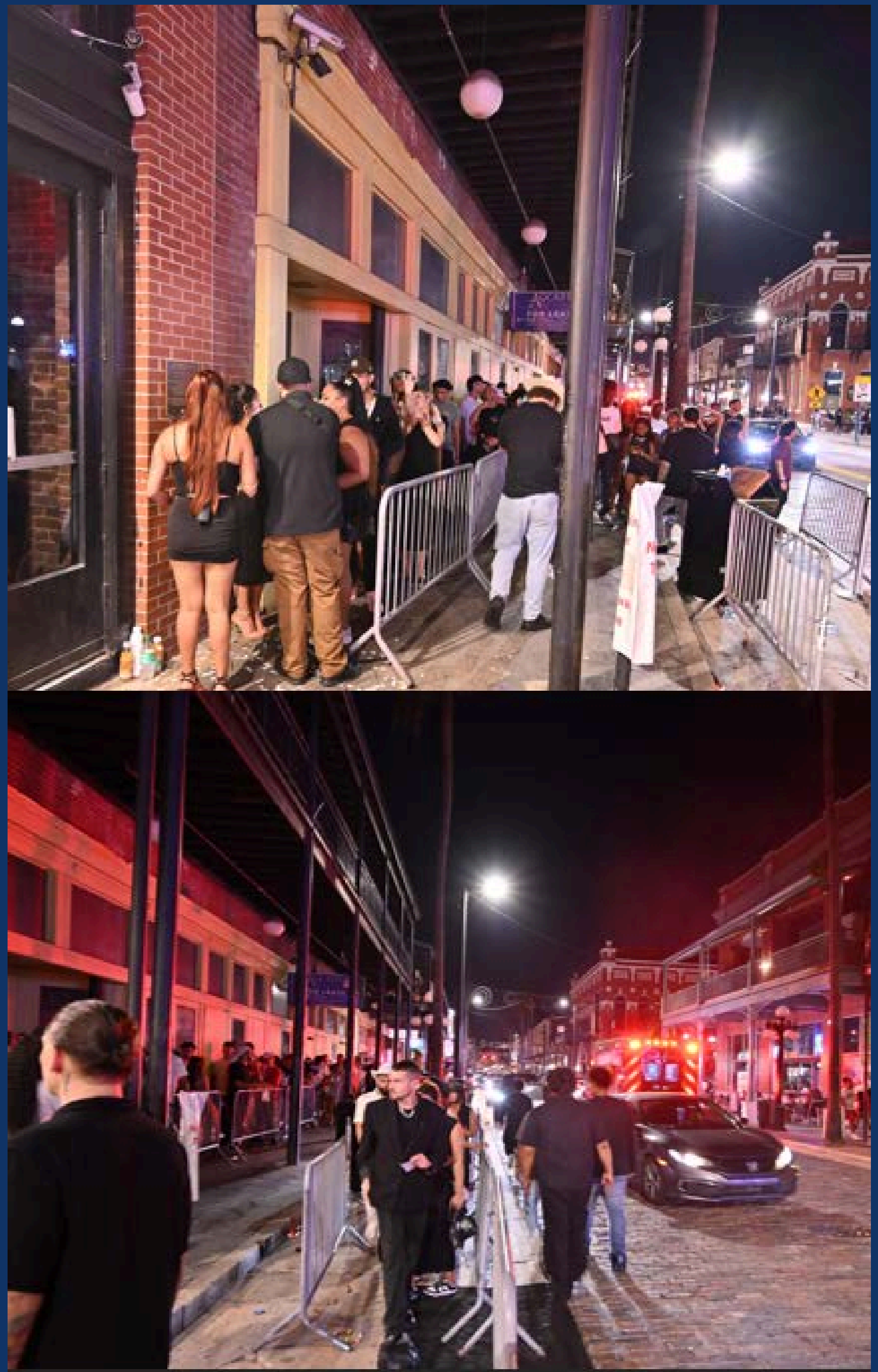
- Pathways/Entry: Clearly define and light paths for visitors. Access to non-public areas (offices, storage) should be easily restricted (e.g., locked doors, card access).

- Perimeter: Property boundaries should be clear—fencing, etc.

- Doorways—controlled entry/exit



CONTROLLED & UNOBSTRUCTED



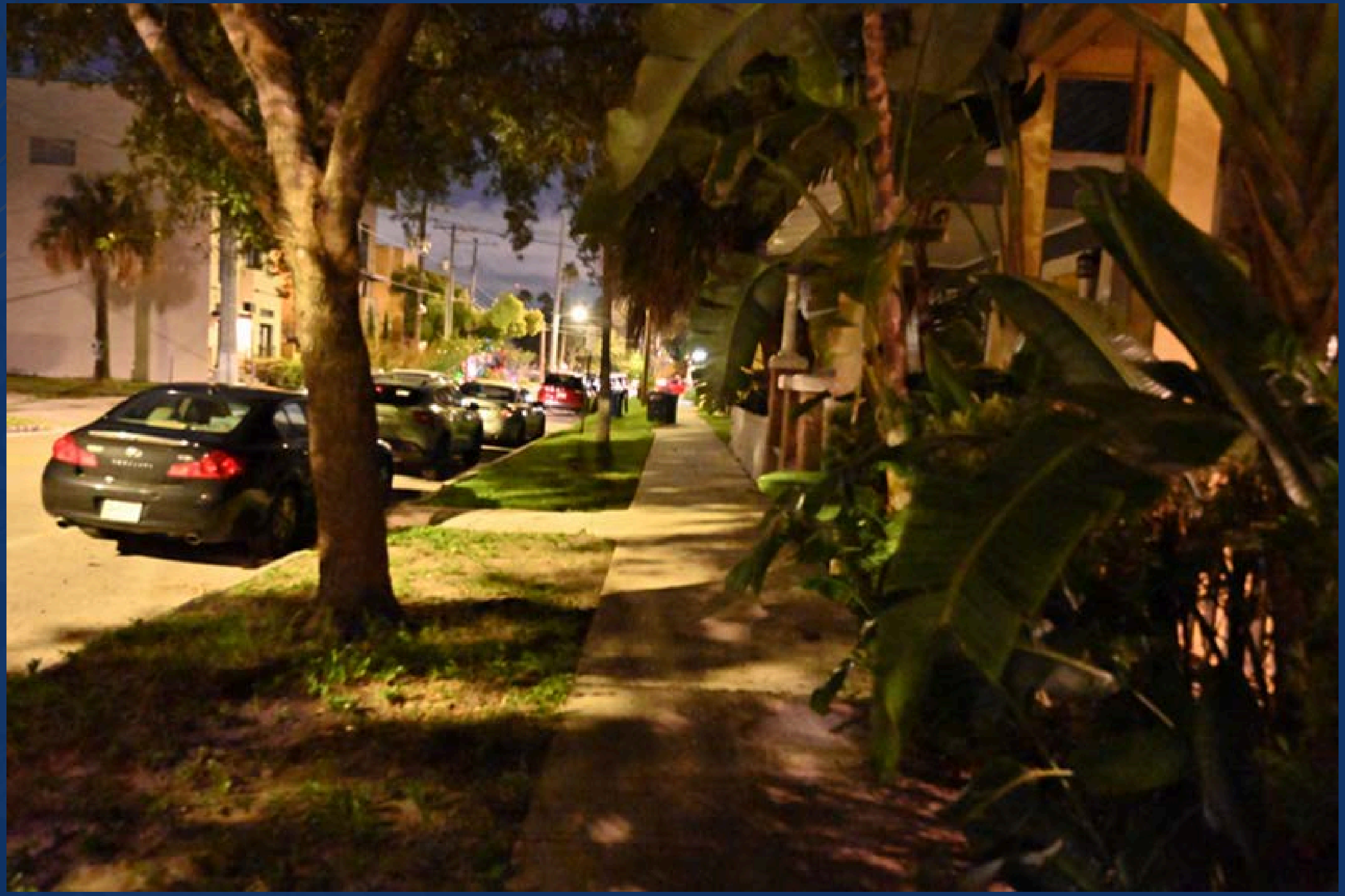
OVERCROWDED & OBSTRUCTED

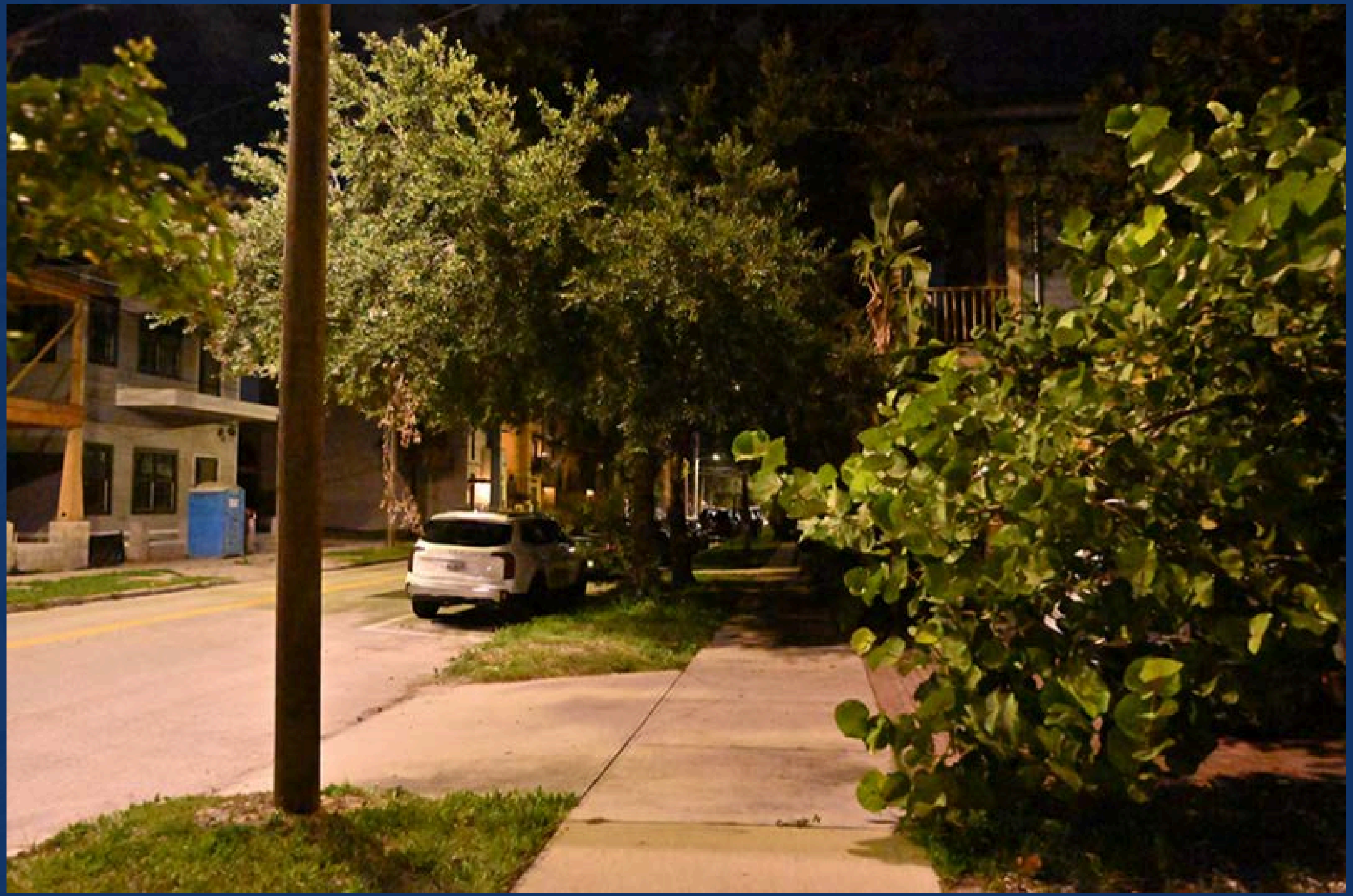
TERRITORIAL REINFORCEMENT

(Ownership & Discouraging Trespass)

- **Boundaries & Maintenance:** Clearly define property lines (landscaping, low fencing). A well-maintained property signals active use and discourages trespass. Prompt repairs and general tidiness are key.]

- **Signage:** Post clear directional signage for visitors. Consider "No Trespassing" or "Private Property" signs for non-public or vulnerable access areas. Emergency contact information should be clearly posted.





3. DEVELOP & PRACTICE A PLAN

- Create security & emergency action plans (discuss options for security / security teams)

- Educate applicable personnel

- Practice the plan to ensure familiarity & identify any shortcomings

4. INFORM & EDUCATE GREETERS *(and other key personnel)*

○ The power of “Hello”

○ Identify suspicious behavior

Recognize signs, report immediately—internal or external

5. PURSUE GRANTS

- The federal government offers a variety of grants and other assistance—see resources

6. REPORT OFFENSES & SUSPICIOUS ACTIVITY

- See Something?
    - ***Say Something!***

It’s not a slogan,
It is the first step in shared safety!

IF YOU SEE SOMETHING, SAY SOMETHING!

SUSPICIOUS PERSON OR ACTIVITY:

- **Internal Reporting:** Immediately inform your designated leaders or security team members about the observation.
- **Emergency:** If immediate threat, call **911**
- **Non-Emergency:** If the activity is suspicious but not immediately life-threatening, call our non-emergency number: **813-231-6130**

- Focus on **behavior** and gather **details** -

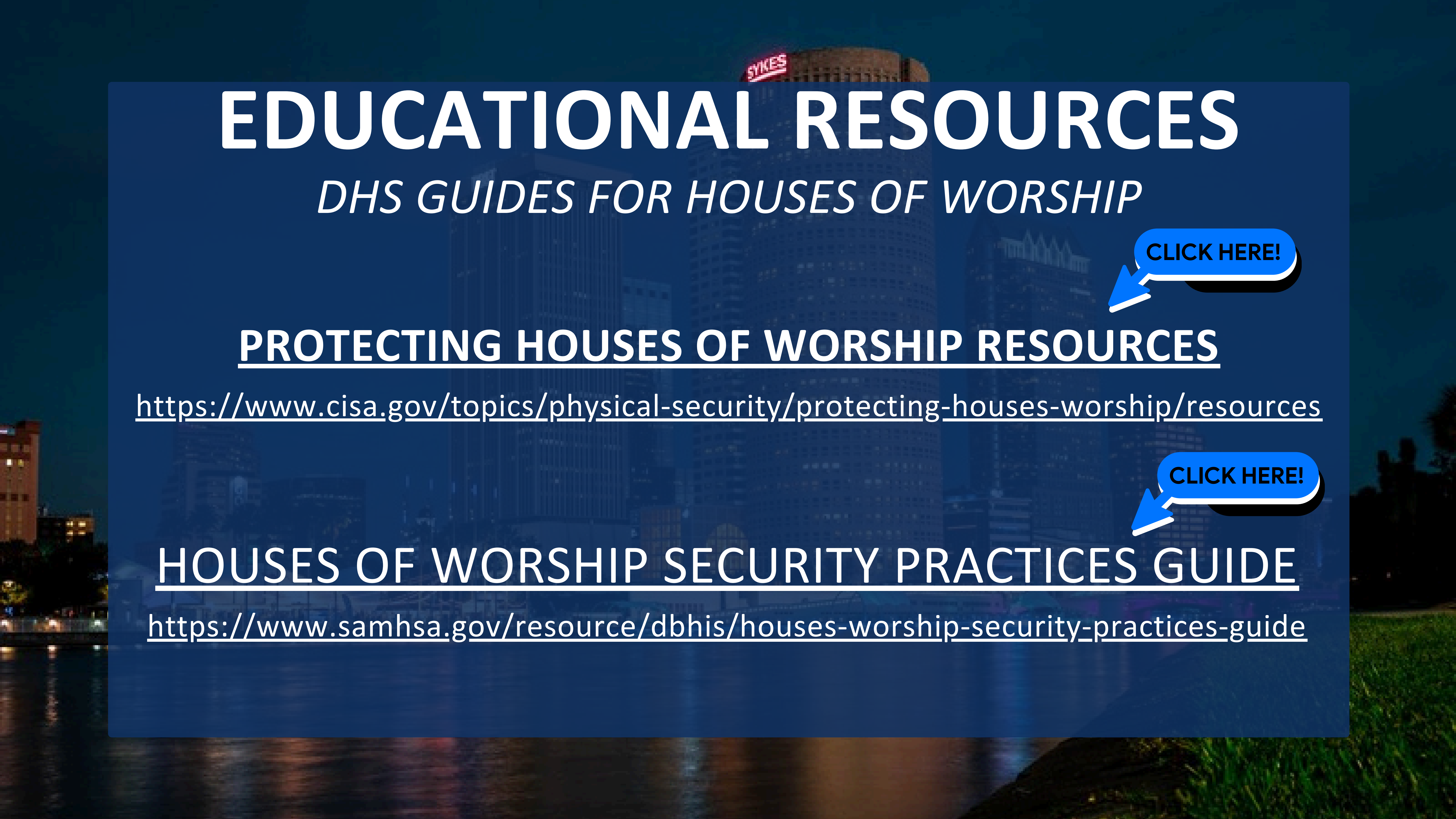
POSSIBLE SUSPICIOUS BEHAVIORS OR THREAT INDICATORS

THREATS/BEHAVIORS	ACTION STEPS TO CONSIDER
Individuals conducting unauthorized photography or video recording of entry points, security cameras or layouts	Observe, document and report suspicious behavior to your security personnel or TPD
Unusual interest in building schedules, leadership routines or crowd sizes	Enhance awareness among staff and congregants through regular safety briefings
Loitering or unfamiliar vehicles parked nearby for extended periods	Observe, document and report suspicious behavior to security personnel or TPD
Attempts to access restricted areas or bring in large, unexplained packages	Attempt to identify - inconsistent stores or evasive answers when questioned by staff or security require additional involvement from security personnel or Tampa PD.
Trust your instincts	<u>See Something, Say Something:</u> If you do not feel safe, or something makes you feel uneasy, call the Tampa Police Department. If you believe something is life-threatening, or a crime is in progress, call 911!

AIDING RESPONDING LAW ENFORCEMENT

- Be as descriptive as possible to 911—Number of offenders, location, clothing, weapons, physical, vehicles, etc.
- Keep hands visible & empty, no sudden movements, follow directions
- Help direct officers—layout, access to areas (keys, etc.)
- Inform officers of any special threats or concerns
- Exit area
- Post-event considerations

GET INVOLVED & STAY INFORMED



EDUCATIONAL RESOURCES

DHS GUIDES FOR HOUSES OF WORSHIP

CLICK HERE!

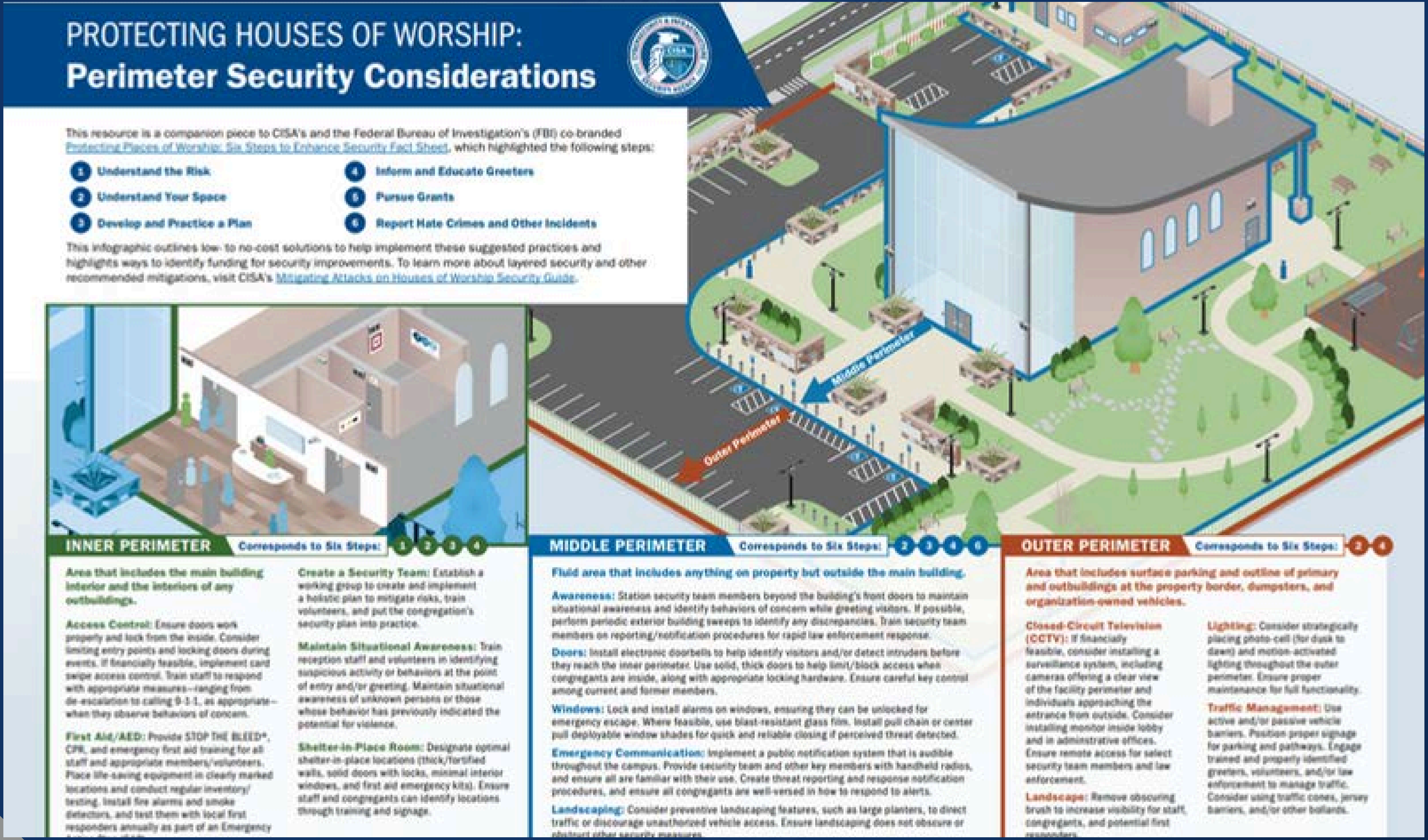
PROTECTING HOUSES OF WORSHIP RESOURCES

https://www.cisa.gov/topics/physical-security/protecting-houses-worship/resources

CLICK HERE!

HOUSES OF WORSHIP SECURITY PRACTICES GUIDE

https://www.samhsa.gov/resource/dbhis/houses-worship-security-practices-guide


Middle Perimeter
Outer Perimeter

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.

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

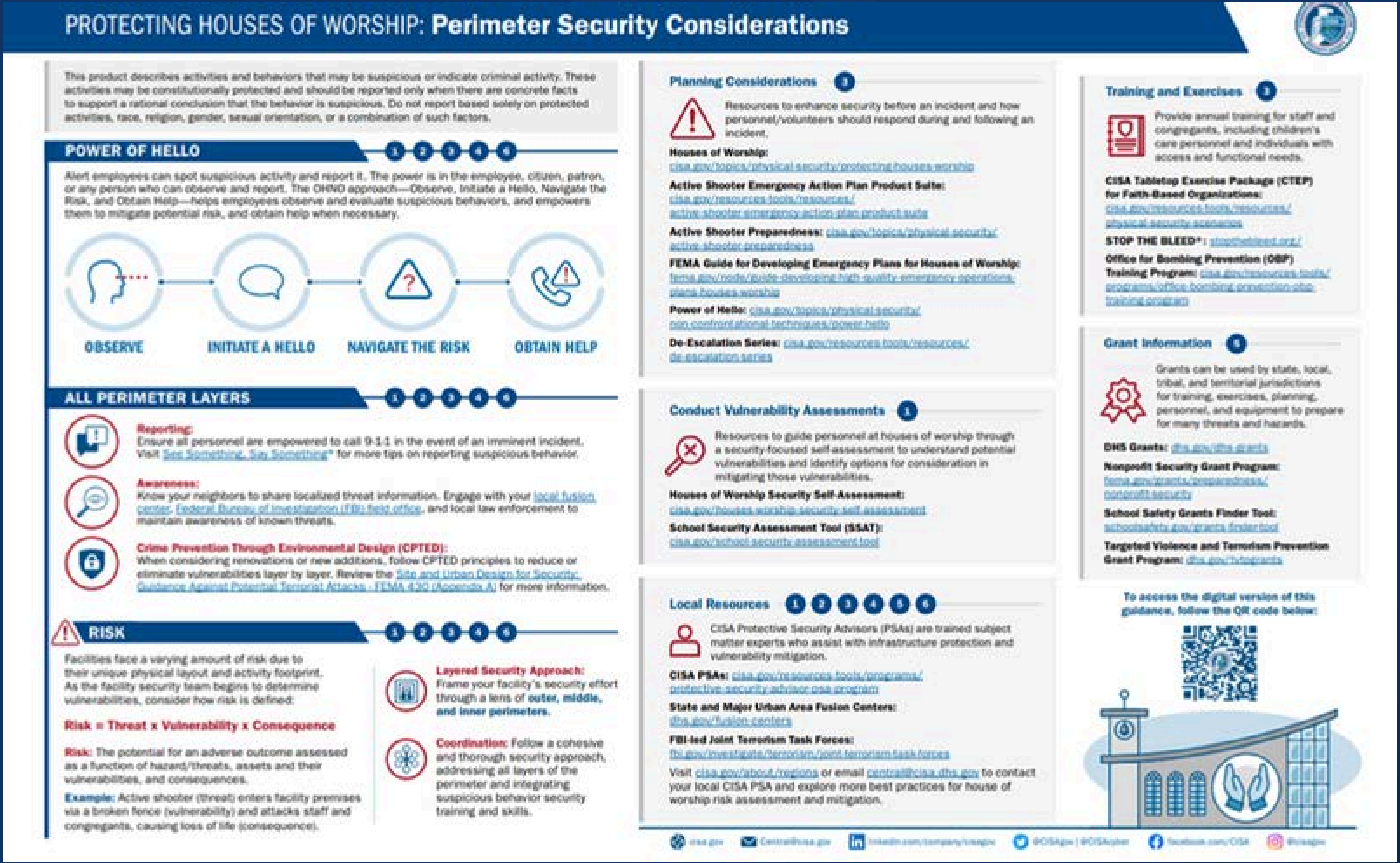
Area that includes surface parking and outline of primary and outbuildings at the property border, dumpsters, and organization-owned vehicles.

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 administrative 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.



PROTECTING HOUSES OF WORSHIP: **Perimeter Security Considerations**

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.

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 6

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

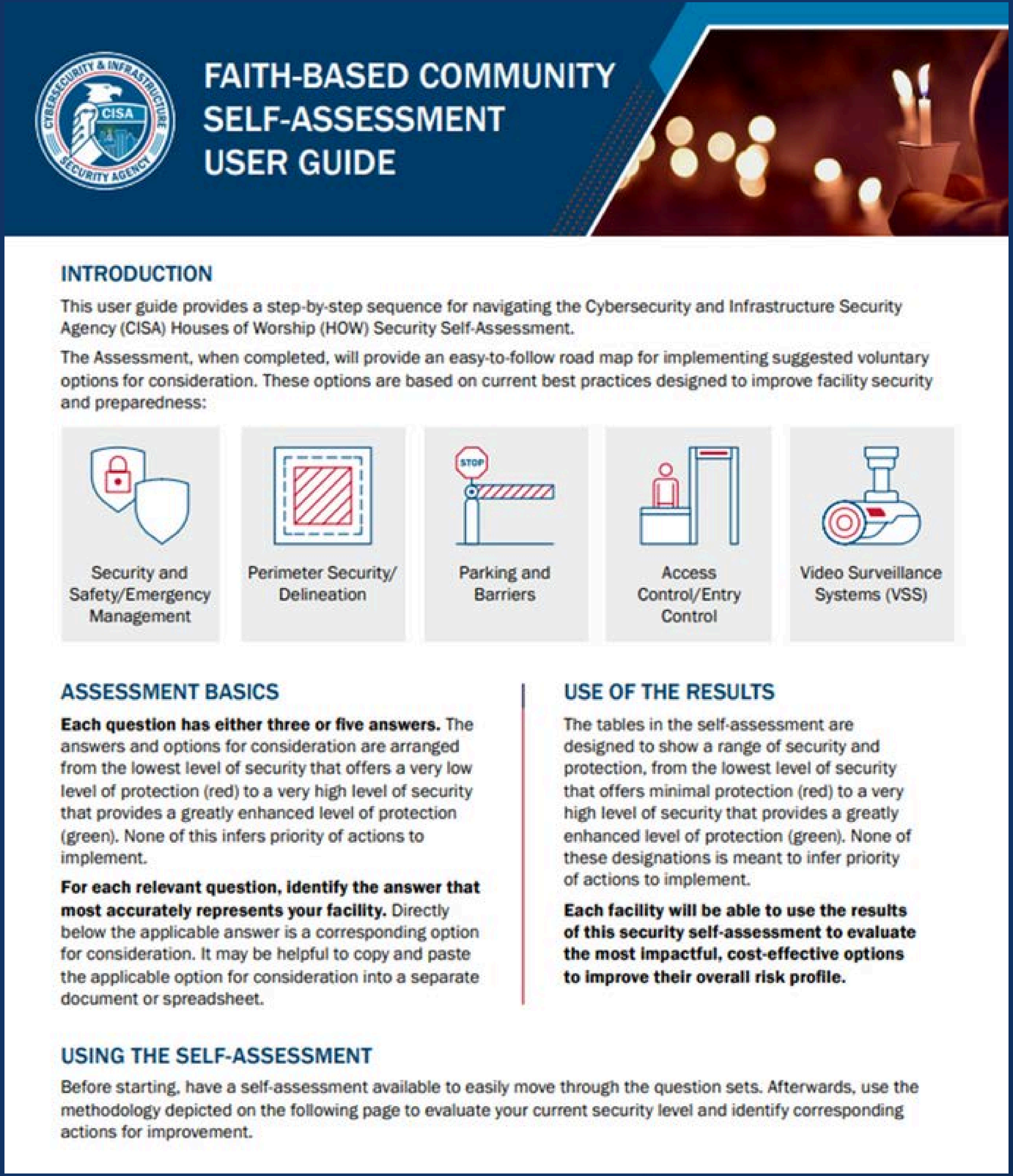
Nonprofit Security Grant Program:
fema.gov/grants/preparedness/nonprofit-security

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

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

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

cisa.gov Central@cisa.gov linkedin.com/company/cisagov @CISAgov | @CISAcyber facebook.com/CISA @cisagov



FAITH-BASED COMMUNITY SELF-ASSESSMENT USER GUIDE

INTRODUCTION

This user guide provides a step-by-step sequence for navigating the Cybersecurity and Infrastructure Security Agency (CISA) Houses of Worship (HOW) Security Self-Assessment.

The Assessment, when completed, will provide an easy-to-follow road map for implementing suggested voluntary options for consideration. These options are based on current best practices designed to improve facility security and preparedness:

- Security and Safety/Emergency Management
- Perimeter Security/ Delineation
- Parking and Barriers
- Access Control/Entry Control
- Video Surveillance Systems (VSS)

ASSESSMENT BASICS

Each question has either three or five answers. The answers and options for consideration are arranged from the lowest level of security that offers a very low level of protection (red) to a very high level of security that provides a greatly enhanced level of protection (green). None of this infers priority of actions to implement.

For each relevant question, identify the answer that most accurately represents your facility. Directly below the applicable answer is a corresponding option for consideration. It may be helpful to copy and paste the applicable option for consideration into a separate document or spreadsheet.

USE OF THE RESULTS

The tables in the self-assessment are designed to show a range of security and protection, from the lowest level of security that offers minimal protection (red) to a very high level of security that provides a greatly enhanced level of protection (green). None of these designations is meant to infer priority of actions to implement.

Each facility will be able to use the results of this security self-assessment to evaluate the most impactful, cost-effective options to improve their overall risk profile.

USING THE SELF-ASSESSMENT

Before starting, have a self-assessment available to easily move through the question sets. Afterwards, use the methodology depicted on the following page to evaluate your current security level and identify corresponding actions for improvement.

EDUCATIONAL RESOURCES

developed by the FBI & Homeland Security

CLICK HERE!

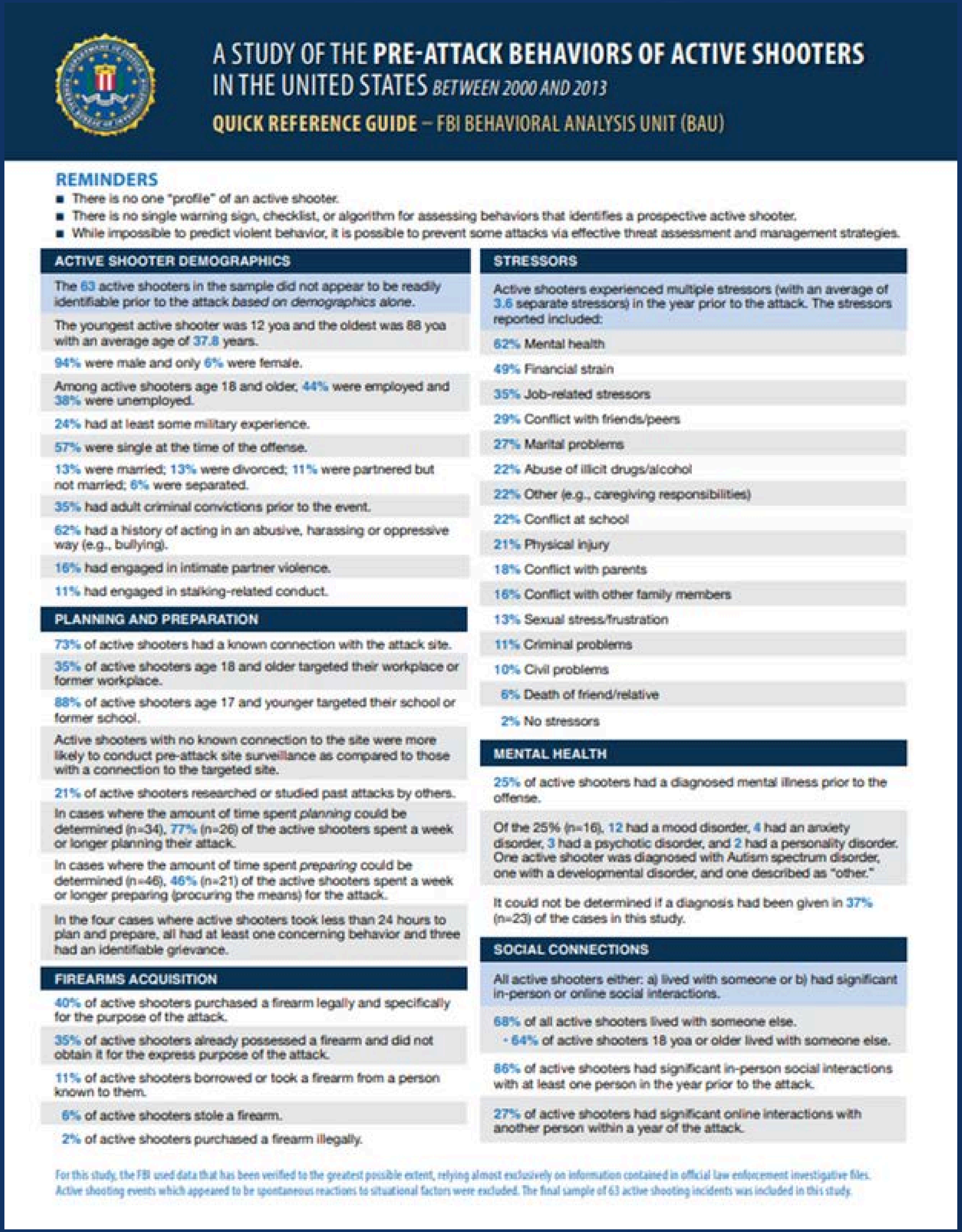
FBI ACTIVE SHOOTER SAFETY RESOURCES

https://www.fbi.gov/how-we-can-help-you/active-shooter-safety-resources

ATTACKS IN CROWDED AND PUBLIC SPACES

CLICK HERE!

https://www.ready.gov/public-spaces



A STUDY OF THE **PRE-ATTACK BEHAVIORS OF ACTIVE SHOOTERS** IN THE UNITED STATES *BETWEEN 2000 AND 2013*

QUICK REFERENCE GUIDE – FBI BEHAVIORAL ANALYSIS UNIT (BAU)

REMINDERS

- There is no one "profile" of an active shooter.
- There is no single warning sign, checklist, or algorithm for assessing behaviors that identifies a prospective active shooter.
- While impossible to predict violent behavior, it is possible to prevent some attacks via effective threat assessment and management strategies.

ACTIVE SHOOTER DEMOGRAPHICS

The 63 active shooters in the sample did not appear to be readily identifiable prior to the attack *based on demographics alone.*

The youngest active shooter was 12 yoa and the oldest was 88 yoa with an average age of 37.8 years.

94% were male and only 6% were female.

Among active shooters age 18 and older, 44% were employed and 38% were unemployed.

24% had at least some military experience.

57% were single at the time of the offense.

13% were married; 13% were divorced; 11% were partnered but not married; 6% were separated.

35% had adult criminal convictions prior to the event.

62% had a history of acting in an abusive, harassing or oppressive way (e.g., bullying).

16% had engaged in intimate partner violence.

11% had engaged in stalking-related conduct.

PLANNING AND PREPARATION

73% of active shooters had a known connection with the attack site.

35% of active shooters age 18 and older targeted their workplace or former workplace.

88% of active shooters age 17 and younger targeted their school or former school.

Active shooters with no known connection to the site were more likely to conduct pre-attack site surveillance as compared to those with a connection to the targeted site.

21% of active shooters researched or studied past attacks by others.

In cases where the amount of time spent *planning* could be determined (n=34), 77% (n=26) of the active shooters spent a week or longer planning their attack.

In cases where the amount of time spent *preparing* could be determined (n=46), 46% (n=21) of the active shooters spent a week or longer preparing (procuring the means) for the attack.

In the four cases where active shooters took less than 24 hours to plan and prepare, all had at least one concerning behavior and three had an identifiable grievance.

FIREARMS ACQUISITION

40% of active shooters purchased a firearm legally and specifically for the purpose of the attack.

35% of active shooters already possessed a firearm and did not obtain it for the express purpose of the attack.

11% of active shooters borrowed or took a firearm from a person known to them.

6% of active shooters stole a firearm.

2% of active shooters purchased a firearm illegally.

STRESSORS

Active shooters experienced multiple stressors (with an average of 3.6 separate stressors) in the year prior to the attack. The stressors reported included:

62%	Mental health
49%	Financial strain
35%	Job-related stressors
29%	Conflict with friends/peers
27%	Marital problems
22%	Abuse of illicit drugs/alcohol
22%	Other (e.g., caregiving responsibilities)
22%	Conflict at school
21%	Physical injury
18%	Conflict with parents
16%	Conflict with other family members
13%	Sexual stress/frustration
11%	Criminal problems
10%	Civil problems
6%	Death of friend/relative
2%	No stressors

MENTAL HEALTH

25% of active shooters had a diagnosed mental illness prior to the offense.

Of the 25% (n=16), 12 had a mood disorder, 4 had an anxiety disorder, 3 had a psychotic disorder, and 2 had a personality disorder. One active shooter was diagnosed with Autism spectrum disorder, one with a developmental disorder, and one described as "other."

It could not be determined if a diagnosis had been given in 37% (n=23) of the cases in this study.

SOCIAL CONNECTIONS

All active shooters either: a) lived with someone or b) had significant in-person or online social interactions.

68% of all active shooters lived with someone else.
- 64% of active shooters 18 yoa or older lived with someone else.

86% of active shooters had significant in-person social interactions with at least one person in the year prior to the attack.

27% of active shooters had significant online interactions with another person within a year of the attack.

For this study, the FBI used data that has been verified to the greatest possible extent, relying almost exclusively on information contained in official law enforcement investigative files. Active shooting events which appeared to be spontaneous reactions to situational factors were excluded. The final sample of 63 active shooting incidents was included in this study.

EDUCATIONAL RESOURCES

FEDERAL EMERGENCY MANAGEMENT AGENCY

FAITH-BASED & VOLUNTEER PARTNERSHIP RESOURCES

https://www.fema.gov/emergency-managers/individuals-communities/faith-volunteer

CLICK HERE!

FEMA GRANTS

https://www.fema.gov/grants

CLICK HERE!

If you have additional questions or would like a security walk-through of your house of worship, email our Community Engagement Bureau

TPD-CommunityEngagement@tampa.gov

THANK YOU!!