CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

ACTIVE SHOOTER PLANNING & PREPAREDNESS

PHYSICAL SECURITY CONSIDERATIONS

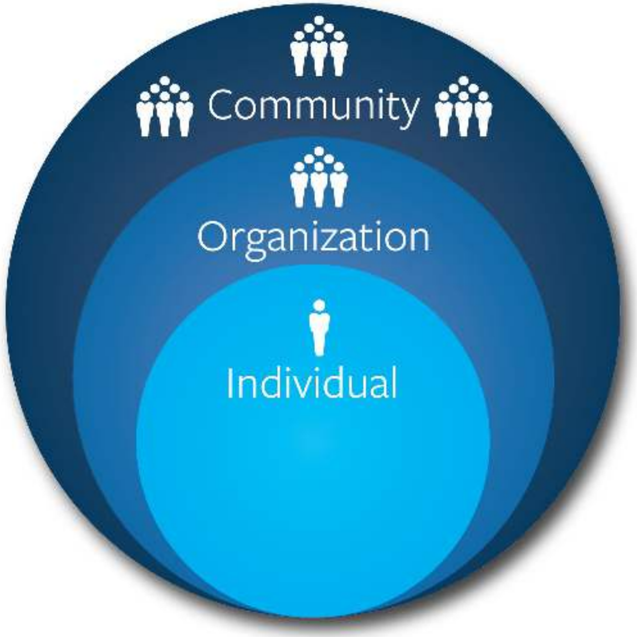
CISA Region 8
Mar 9, 2023

Disclaimer

- This presentation and the accompanying documents describe activities and behaviors that may be concerning or possibly indicative of impending violence.
- Only report when there are sufficient facts to support a rational conclusion that the behavior or activity represents a potential threat of violence and not based solely on race, religion, gender, sexual orientation, age, disability, or a combination of only such factors.
- The approaches, techniques, and tactics described in this presentation and the accompanying documents are options for consideration. They are not intended to mandate policy or direct any action.
- DHS assumes no liability for any injuries associated with the implementation of this training.

Goals

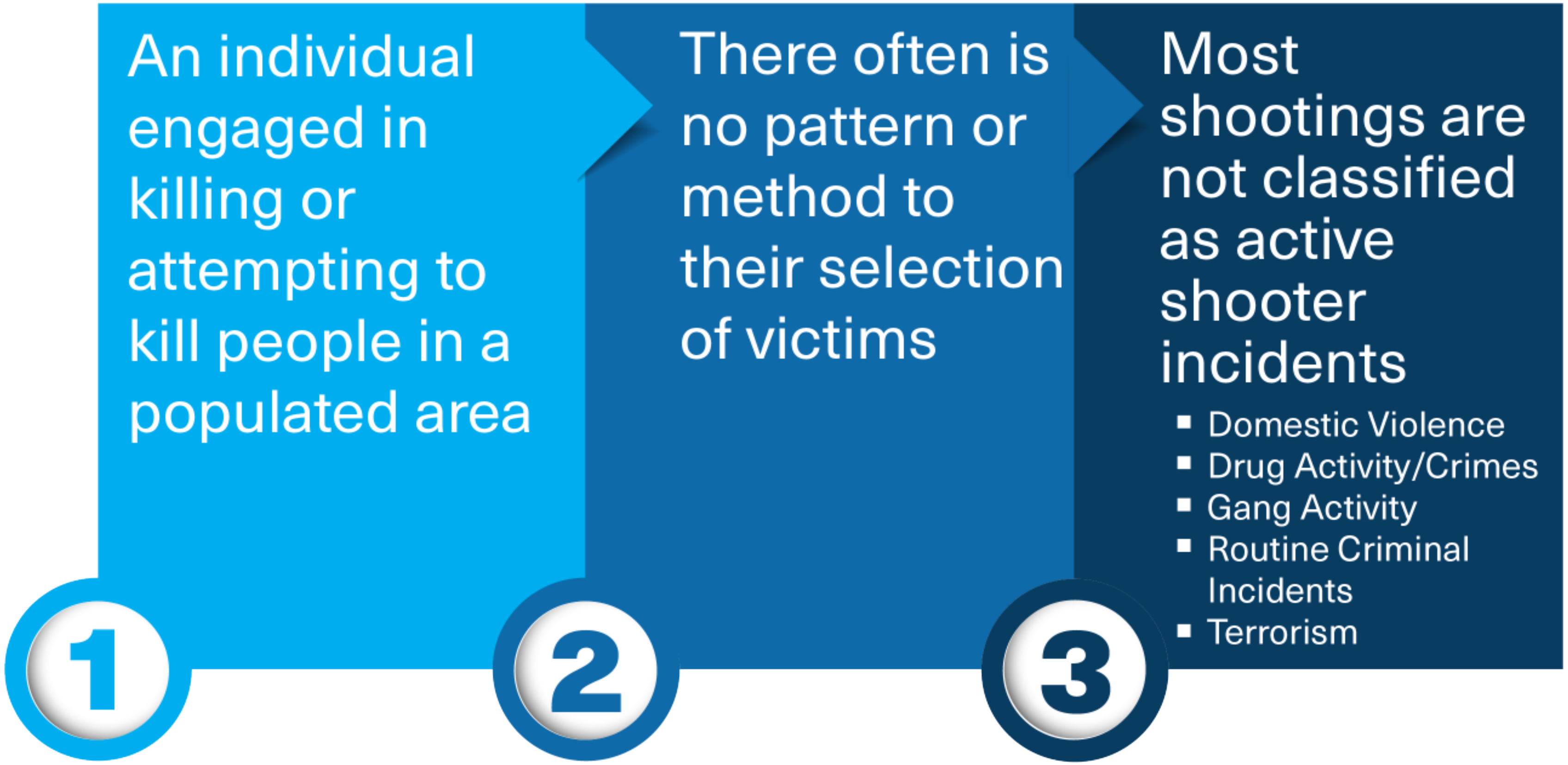
- ✓ **Recognition**
  understand the threat
- ✓ **Prevention**
  recognize, report, intervene
- ✓ **Preparedness**
  plan for response and recovery



Threat Vectors

- Active Shooter
- Vehicle Ramming
- Insider Threat
- Edged Weapon Attack
- Improvised Explosive Device (IED)
- Fire as a Weapon
- Small Unmanned Aircraft Systems (sUAS)
- Complex Coordinated Attack (CCA)

Active Shooter



1

An individual engaged in killing or attempting to kill people in a populated area

2

There often is no pattern or method to their selection of victims

3

Most shootings are not classified as active shooter incidents

- Domestic Violence
- Drug Activity/Crimes
- Gang Activity
- Routine Criminal Incidents
- Terrorism

Active Shooter Trends

Active Shooter Incidents 2017–2021

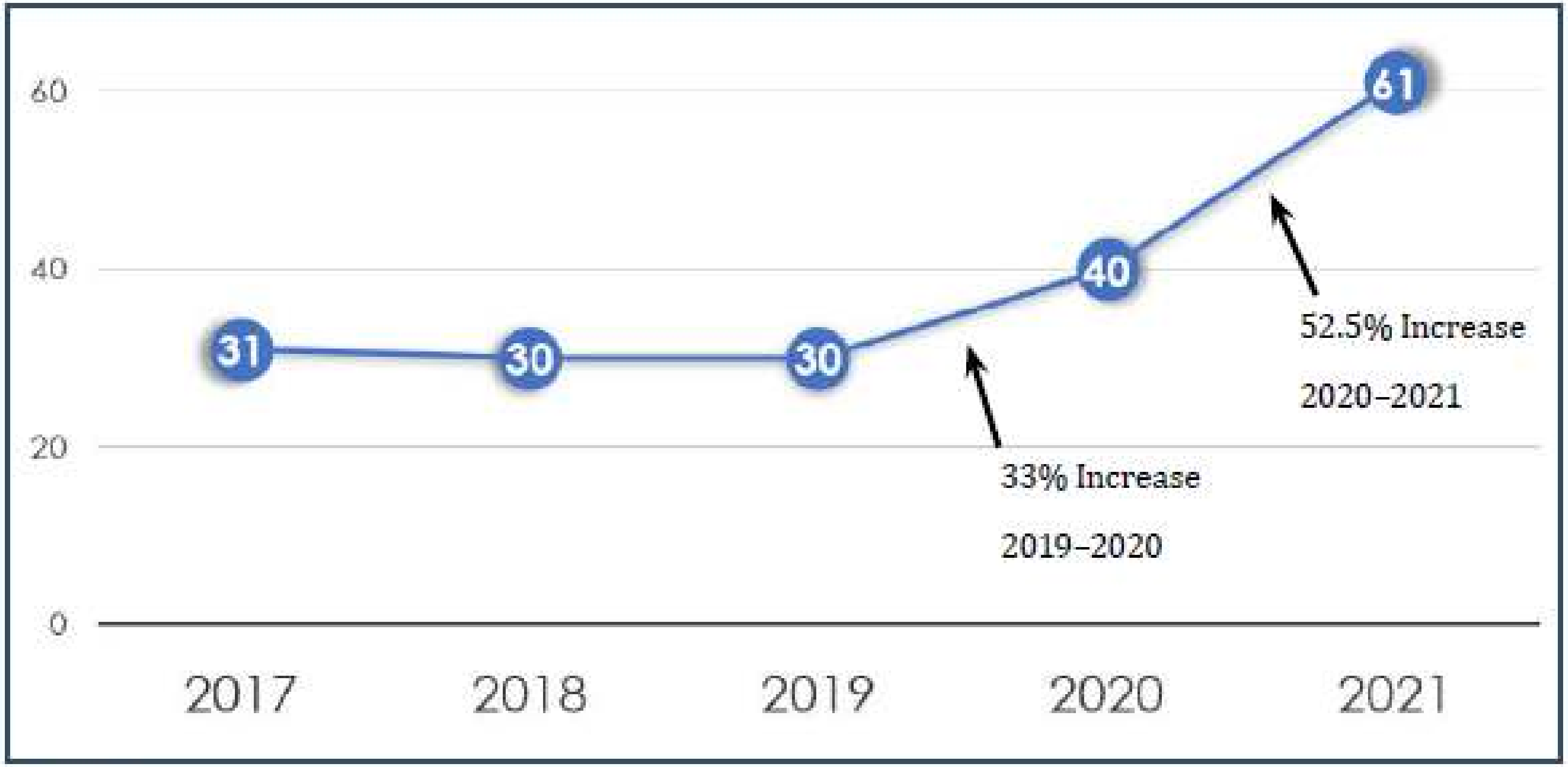
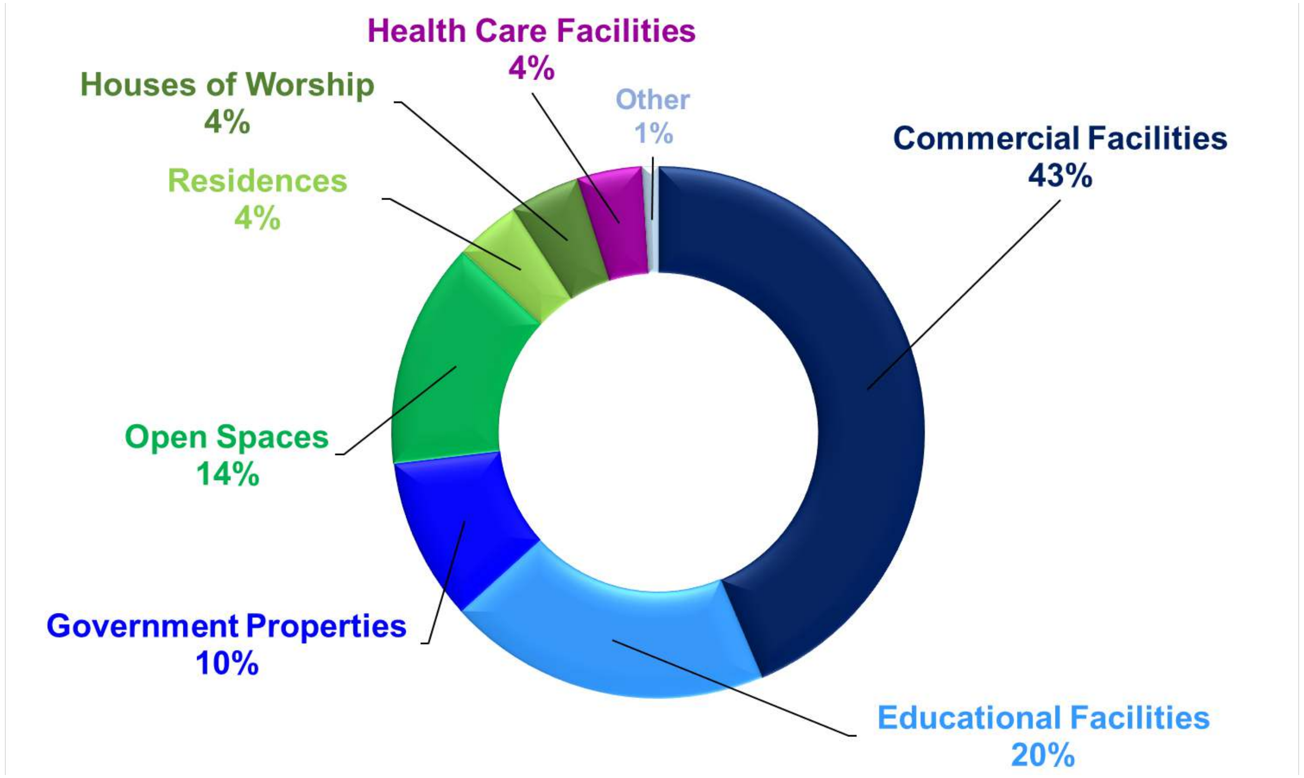


Figure 1

FBI Report: *Active Shooter Incidents in the United States in 2021*

Incident Locations

A study of 305 Active Shooter Incidents in the U.S. between 2000 and 2019



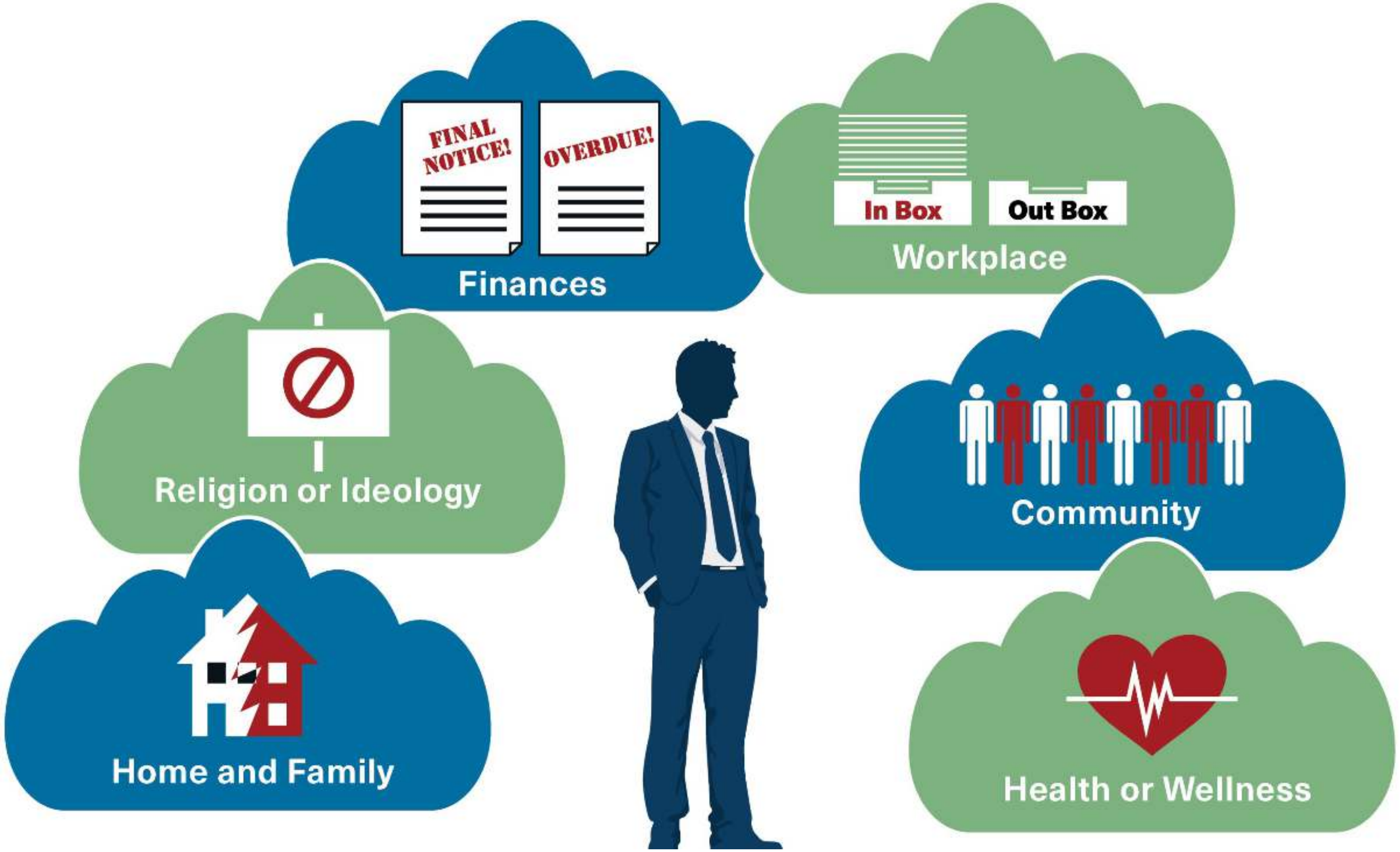
FBI Law Enforcement Bulletin. *Active Shooter Events from 2000 to 2013, Active Shooter Incidents in the United States in 2014 and 2015, 2016 and 2017, 2018, 2019*

Active Shooter Prevention

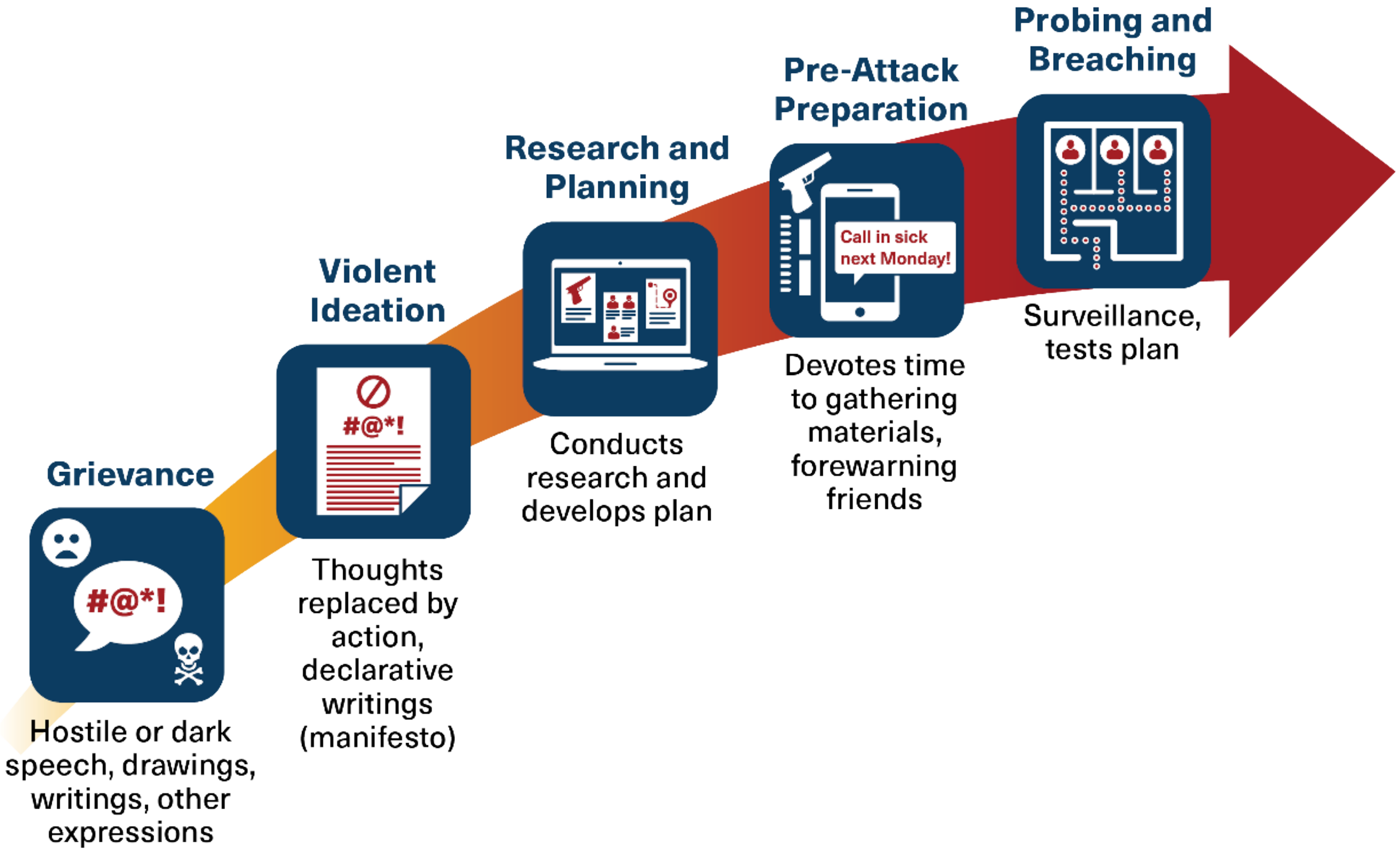
- ✓ **Train** employees to recognize behaviors on the *Pathway to Violence*.
- ✓ **Instill** a positive culture for reporting.
- ✓ **Develop** intervention capabilities.

Awareness + Action = Prevention

Behavioral Change Indicators



Pathway to Violence



Grievance

Hostile or dark speech, drawings, writings, other expressions

Violent Ideation

Thoughts replaced by action, declarative writings (manifesto)

Research and Planning

Conducts research and develops plan

Pre-Attack Preparation

Devotes time to gathering materials, forewarning friends

Probing and Breaching

Surveillance, tests plan

Incorporate Security Measures

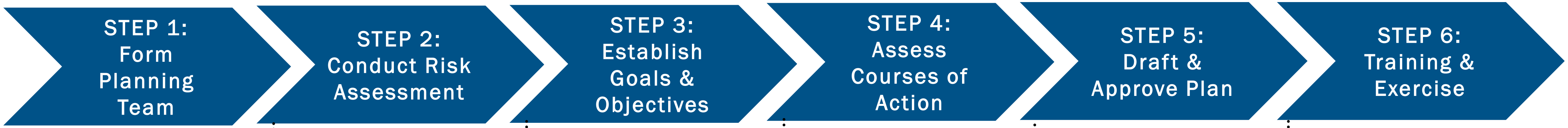
- ✓ Determine if a **security plan** exists for the facility and if current protective measures provide sufficient security.

- ✓ Conduct a **vulnerability assessment** to identify and prioritize areas of concern.

- ✓ Develop an **emergency action plan** – specify steps venue personnel should take if faced with an incident.
  - Coordinate/exercise plan with local law enforcement and first responders
  - Train employees on life saving techniques – “Stop the Bleed,” “You are the help until help arrives”

- ✓ Implement appropriate measures to address potential gaps in security identified by the vulnerability assessment

Create an Emergency Action Plan



STEP 1: Form Planning Team

- Identify Core Planning Team
- Form a Common Framework
- Define and Assign Roles
- Determine a Meeting Schedule

STEP 2: Conduct Risk Assessment

- Identify Threats
- Assess Risk
- Prioritize Risk

STEP 3: Establish Goals & Objectives

- Develop Goals
- Develop Objectives

STEP 4: Assess Courses of Action

- Identify Courses of Action
- Identify Resources
- Assign COAs to Positions

STEP 5: Draft & Approve Plan

- Format the Plan
- Write the Plan
- Review the Plan
- Approve and Share the Plan

STEP 6: Training & Exercise

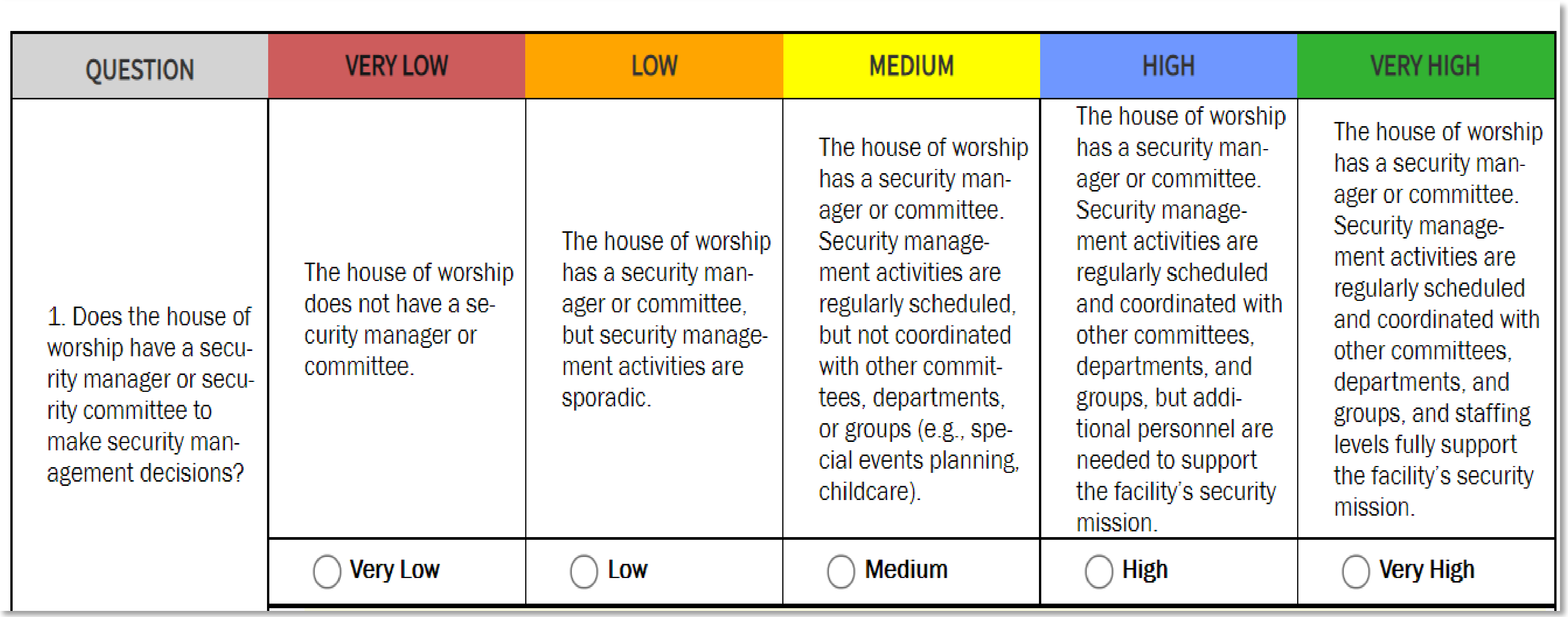
- Train Stakeholders
- Exercise the Plan
- Review, Revise, and Maintain the Plan

Sources:

1. U.S. Interagency Security Committee. 2015. *Facility Security Plan: An Interagency Security Committee Guide*. Feb. 2015. cisa.gov/sites/default/files/publications/ISC-Facility-Security-Plan-Guide-2015-508.pdf.
2. Cybersecurity and Infrastructure Security Agency. 2021. *CHEMLOCK: Secure Your Chemicals*. November 2021. cisa.gov/sites/default/files/publications/chemlock-secure-chems-nov21-508.pdf.
3. U.S. Department of Homeland Security. n.d. *Emergency Action Plan Guide: Active Shooter Preparedness*. Accessed Sep. 21, 2022. cisa.gov/sites/default/files/publications/active-shooter-emergency-action-plan-112017-508v2.pdf.

Self-Assessment Tool

An **easy to use, interactive, security-focused self-assessment** tool that assists stakeholders in understanding potential risks and identifying corresponding risk mitigation solutions.



QUESTION	VERY LOW	LOW	MEDIUM	HIGH	VERY HIGH
1. Does the house of worship have a security manager or security committee to make security management decisions?	The house of worship does not have a security manager or committee.	The house of worship has a security manager or committee, but security management activities are sporadic.	The house of worship has a security manager or committee. Security management activities are regularly scheduled, but not coordinated with other committees, departments, or groups (e.g., special events planning, childcare).	The house of worship has a security manager or committee. Security management activities are regularly scheduled and coordinated with other committees, departments, and groups, but additional personnel are needed to support the facility's security mission.	The house of worship has a security manager or committee. Security management activities are regularly scheduled and coordinated with other committees, departments, and groups, and staffing levels fully support the facility's security mission.
	○ Very Low	○ Low	○ Medium	○ High	○ Very High

cisa.gov/houses-of-worship

Self-Assessment Tool

Results of the assessment can **assist organizations in improving security and managing identified risks** through the ability to:

- **Prioritize** potential security measures
- **Review best practices** and available resources
- **Develop investment justifications** for internal budgeting processes or external grant requests

cisa.gov/houses-of-worship

Risk Mitigation

Based upon the results of the vulnerability assessment, operators can consider some of the below cost-effective protective measures to enhance security:

- Post appropriate way-finding and accessibility signage on entrances and paths
- Ensure CCTV systems are operable and monitored
- Restrict high-speed avenues of approach; have appropriate lighting
- Limit amount of people at entry point
- Ensure support personnel are familiar with de-escalation tactics; use “buddy system”

Risk Mitigation

Based upon the results of the vulnerability assessment, operators can consider some of the below cost-effective protective measures to enhance security:

- Secure or post workers to monitor non-public entrances
- Consider measures related to access control/bag check procedures
- Ensure a clean perimeter area; remove/lock trash receptacles
- Establish several communication methods with local LE for reporting
- Train support personnel to report suspicious bags, parcels or cookware to local LE
- Secure chemicals that could pose risks

Planning Resources

Mitigating Attacks on Houses of Worship Security Guide

CISA developed a security framework that can be tailored to houses of worship of all sizes and denominations
cisa.gov/faith-based-organizations-houses-worship

Active Shooter Emergency Action Plan Template

CISA developed the Emergency Action Plan (EAP) template which documents information recommended for an effective EAP to help organizations prepare their personnel for and respond to active shooter incidents.
cisa.gov/active-shooter-emergency-action-plan-trailer-and-video

Resources related to planning

- Georgia Emergency Operations Plan Template
- ready.gov/business-continuity-plan
- FEMA Planning Guides
- Guide for Developing High-Quality Emergency Operations Plans for Houses of Worship
- New Hampshire Resource Center – Houses of Worship

If an Incident Occurs

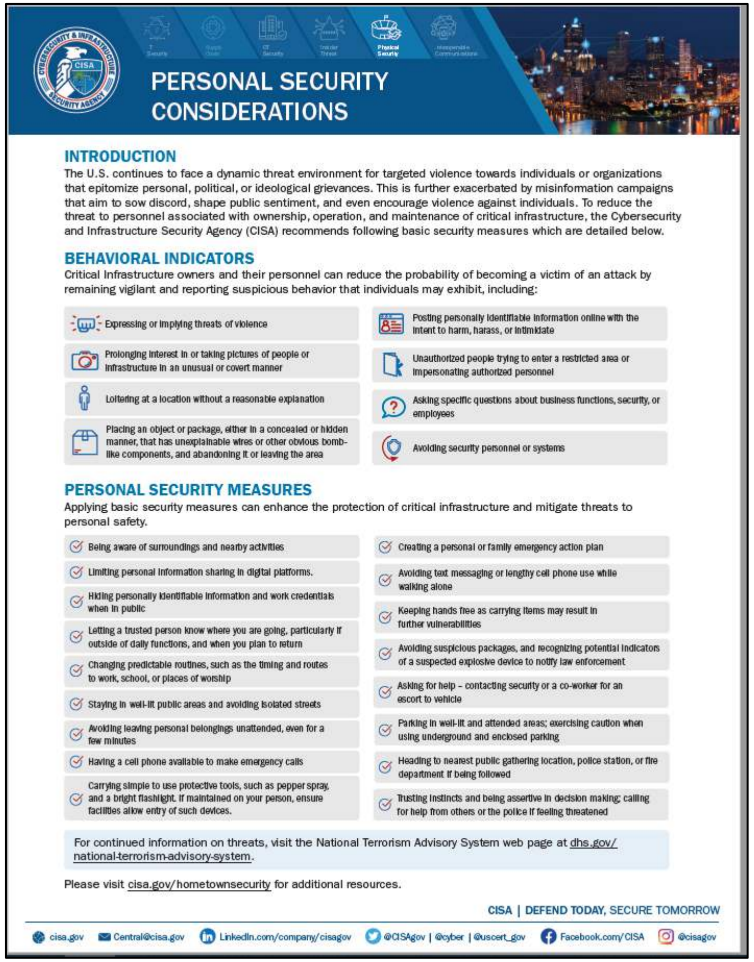
- ☎ Immediately call **9-1-1**
- Set the emergency action plan in motion

Every employee and volunteer should be ready to act – this may include performing life-saving procedures

Personal Security Considerations

- Suggests behavioral indicators that potential attackers may exhibit
- Lists personal security measures critical infrastructure personnel can implement to mitigate vulnerability

cisa.gov/critical-infrastructure-and-businesses



Physical Security

PERSONAL SECURITY CONSIDERATIONS

INTRODUCTION

The U.S. continues to face a dynamic threat environment for targeted violence towards individuals or organizations that epitomize personal, political, or ideological grievances. This is further exacerbated by misinformation campaigns that aim to sow discord, shape public sentiment, and even encourage violence against individuals. To reduce the threat to personnel associated with ownership, operation, and maintenance of critical infrastructure, the Cybersecurity and Infrastructure Security Agency (CISA) recommends following basic security measures which are detailed below.

BEHAVIORAL INDICATORS

Critical Infrastructure owners and their personnel can reduce the probability of becoming a victim of an attack by remaining vigilant and reporting suspicious behavior that individuals may exhibit, including:

- Expressing or implying threats of violence
- Prolonging interest in or taking pictures of people or infrastructure in an unusual or covert manner
- Loitering at a location without a reasonable explanation
- Placing an object or package, either in a concealed or hidden manner, that has unexplainable wires or other obvious bomb-like components, and abandoning it or leaving the area
- Posting personally identifiable information online with the intent to harm, harass, or intimidate
- Unauthorized people trying to enter a restricted area or impersonating authorized personnel
- Asking specific questions about business functions, security, or employees
- Avoiding security personnel or systems

PERSONAL SECURITY MEASURES

Applying basic security measures can enhance the protection of critical infrastructure and mitigate threats to personal safety.

- ✓ Being aware of surroundings and nearby activities
- ✓ Limiting personal information sharing in digital platforms.
- ✓ Hiding personally identifiable information and work credentials when in public
- ✓ Letting a trusted person know where you are going, particularly if outside of daily functions, and when you plan to return
- ✓ Changing predictable routines, such as the timing and routes to work, school, or places of worship
- ✓ Staying in well-lit public areas and avoiding isolated streets
- ✓ Avoiding leaving personal belongings unattended, even for a few minutes
- ✓ Having a cell phone available to make emergency calls
- ✓ Carrying simple to use protective tools, such as pepper spray, and a bright flashlight. If maintained on your person, ensure facilities allow entry of such devices.
- ✓ Creating a personal or family emergency action plan
- ✓ Avoiding text messaging or lengthy cell phone use while walking alone
- ✓ Keeping hands free as carrying items may result in further vulnerabilities
- ✓ Avoiding suspicious packages, and recognizing potential indicators of a suspected explosive device to notify law enforcement
- ✓ Asking for help – contacting security or a co-worker for an escort to vehicle
- ✓ Parking in well-lit and attended areas; exercising caution when using underground and enclosed parking
- ✓ Heading to nearest public gathering location, police station, or fire department if being followed
- ✓ Trusting instincts and being assertive in decision making; calling for help from others or the police if feeling threatened

For continued information on threats, visit the National Terrorism Advisory System web page at dhs.gov/national-terrorism-advisory-system.

Please visit cisa.gov/hometownsecurity for additional resources.

CISA | DEFEND TODAY, SECURE TOMORROW

cisa.gov | Central@cisa.gov | Linkedin.com/company/cisagov | @CISAgov | @cyber | @uscert_gov | Facebook.com/CISA | @cisagov

Behavioral Indicators

Expressed or implied threats of violence

Prolonged interest in or taking pictures of people or infrastructure

Loitering at a location without a reasonable explanation

Placing an object or package in a concealed or hidden manner and abandoning it

Posting personally identifiable information online with intent to harm, harass, or intimidate

Trying to enter a restricted area without authorization

Asking specific questions about business functions or security

Avoiding security personnel or systems

Personal Security Measures

- ✓ Being aware of surroundings and nearby activities
- ✓ Limiting personal information sharing in digital platforms
- ✓ Hiding personally identifiable information and work credentials when in public
- ✓ Letting a trusted person know where you are going and when you will return
- ✓ Changing predictable routines, such as timing and routes to work, school, and worship
- ✓ Staying in well-lit public areas and avoiding isolated streets
- ✓ Avoiding leaving personal belongings unattended
- ✓ Having a cell phone available for emergency calls
- ✓ Carrying a simple protective tool, such as pepper spray and a flashlight

Personal Security Measures (Cont'd)

- ✓ Creating a personal or family emergency plan
- ✓ Avoiding text messaging or lengthy cell phone use while walking alone
- ✓ Keeping hands free, as carrying items may result in further vulnerability
- ✓ Avoiding suspicious packages and recognizing suspected explosive devices
- ✓ Asking for help from security or a co-worker for escort to vehicle
- ✓ Parking in well-lit and attended areas
- ✓ Heading to the nearest public gathering location, police station, or fire department if being followed
- ✓ Trusting instincts and being assertive in decision making; calling for help from others or the police if threatened

AUGMENTING SECURITY THROUGH NON-CONFRONTATIONAL TECHNIQUES

Non-Confrontational Techniques

In addition to traditional protective measures, **non-confrontational techniques can serve as important components of a comprehensive security practice** to mitigate the dynamic threat environment.

These techniques augment security through “softer skills” that can be implemented by security and non-security personnel.

CISA makes available several resources to support stakeholders in building this capability:

Employee Vigilance through the **Power of Hello**

OBSERVE

INITIATE A HELLO

NAVIGATE THE RISK

OBTAIN HELP

Power of Hello – assists in easily identifying observable suspicious behaviors

RECOGNIZE

How You Can Notice the Warning Signs of Violence

KEY POINTS TO REMEMBER

De-Escalation Series – introduces four actions that may be taken if suspicious behavior is present – Recognize, Assess, De-Escalate, and Report – to inform effective prevention and mitigation of violence.

These resources are complimentary to "If You See Something, Say Something®"

Employee Vigilance through the Power of Hello

Promotes vigilance

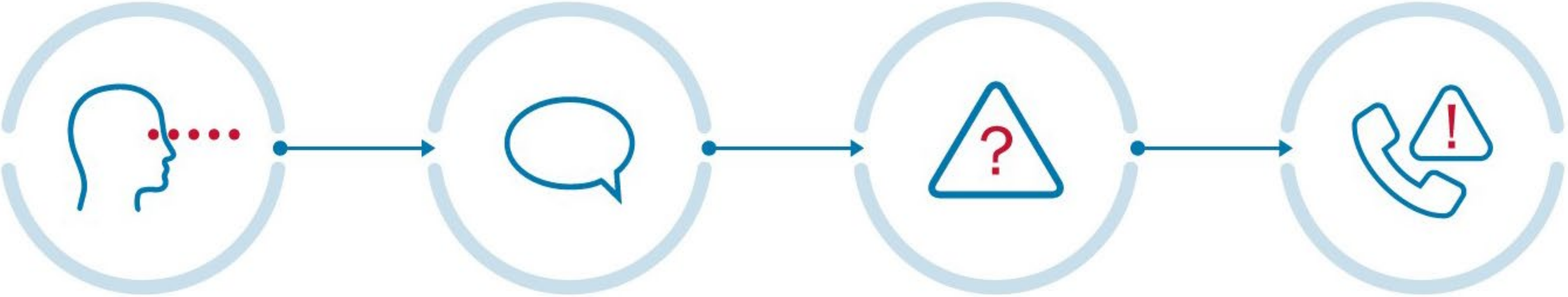
Alert personnel can spot suspicious activity and report it

Power of Hello placemat translated in 18+ languages

cisa.gov/employee-vigilance-power-hello

Employee Vigilance through the Power of Hello

The OHNO approach – **Observe, Initiate a Hello, Navigate the Risk, and Obtain Help** – helps employees observe and evaluate suspicious behaviors, empowers them to mitigate potential risk, and obtain help when necessary.



Observe
Be vigilant of your surroundings

Initiate a Hello
Determine the reason an individual is at your location or facility

Navigate the Risk
Acknowledging a risk can deter a potential threat

Obtain Help
Obtain help from management or authorities

cisa.gov/employee-vigilance-power-hello

Observe

Stay **Vigilant** of your **Surroundings**.

SUSPICIOUS BEHAVIORS:

- Abandoning or placing an object and leaving the area
- Taking pictures/videos of personnel, facilities, security features, or infrastructure in an unusual or covert manner
- Attempting to enter a restricted area or impersonating authorized personnel
- Loitering at a location without a reasonable explanation
- Avoiding security personnel or systems
- Expressing threats of violence

Some activities may be constitutionally protected and should be reported only when there are articulable 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 only such factors.

Initiate a Hello

HELLO

Acknowledging a risk can deter a potential threat.

DO OR SAY THE FOLLOWING:

- Smile, make eye contact, and introduce yourself
- *“Hello. If you need anything, I’ll be right over here.”*
- *“If you are looking for something or someone in particular, I can assist if needed.”*
- *“Hello, if you need assistance I will be around if needed.”*
- *“I will be here in case you need help.”*

Approaching a person viewed as suspicious has potential risks. In some situations, it may be more advisable to report the activity to those with the authority or training to intervene.

Navigate the Risk

Is the **Behavior** you Observed **Threatening** or **Suspicious**?

ASK YOURSELF:

- Do they appear to be legitimately patronizing the location, business, or service?
- Is their clothing consistent with the weather or for the gathering of the day?
- Are they avoiding security?
- Are they asking questions about business functions or employee information?
- Are they causing you to feel threatened?

If you feel threatened, calmly walk away and call 9-1-1

Obtain Help

Obtain help from management or authorities

ANSWER THE FOLLOWING:

Prepare to provide the following information to **first responders**, **security personnel,** or **management officials**:

- What is happening?
- Who is doing it?
- Where is it taking place?
- When did you observe it?
- Why are they here?

Call 9-1-1 for emergencies or if you feel in danger

De-Escalation Series

RECOGNIZE

How You Can Notice the Warning Signs of Violence

Recognize

the warning signs for someone on a path to violence, identify stressors, changes in baseline behavior, and observable behavioral indicators.

ASSESS

How To Navigate the Risk When Someone is Escalating

Assess

the situation to protect personal safety and the safety of those around you. Identify what an escalating person may look like and warning signs.

DE-ESCALATION

How You Can Help Defuse Potentially Violent Situations

De-Escalation

encourages the use of purposeful actions, verbal techniques, and body language to calm a potentially dangerous situation. Safety is the highest priority, know your limits and obtain help immediately if needed.

REPORT

How To Engage Your Organization and Community

Report

concerning behavior or an escalating incident through organizational reporting to enable assessment and management of an evolving threat, and 9-1-1 for immediate threats.

cisa.gov/de-escalation-series

Recognize

People who resort to violence are often driven by a combination of **predispositions, grievances, personal** or **professional stressors,** and **assorted resentments.**

Stressors

Changes

Behavioral Indicators

Observable physical behavioral indicators include, but not limited to:

- Argumentative or uncooperative behaviors
- Clenched jaw and/or balled fists
- Pacing or restlessness
- Trembling or Shaking
- Violating others' personal space
- Making specific threats to inflict harm
- Displaying or making threats to use a weapon

Assess

What Does an Escalating Person Look Like?

Early Warning Signs

- Change in baseline behavior or mood
- Pacing, ruminating, agitated gestures
- Staring through you
- Blocking others’ movement
- Finger pointing
- Distracted or inability to focus

Signs of Imminent Danger

- Flushed, tightened jaw, clenched fists, shaking
- Rapid breathing, raised voice, nervous laughter
- Standing in a position to attack or defend
- Avoiding security systems or personnel
- Abandoning an object or package

De-Escalation: Options to Consider

Use **purposeful actions, verbal communication,** and **body language** techniques to help calm an individual who may be escalating.

Purposeful Actions

- Remain Calm
- Change the Setting
- Respect Personal Space
- Listen
- Empathize

Verbal Communication

Instead Of:	Say…
"Calm down."	"I can see that you are upset…"
"I can't help you."	"I want to help, what can I do?"
"I know how you feel."	"I understand that you feel…"

De-Escalation: Options to Consider

Use **purposeful actions, verbal communication,** and **body language** techniques to help calm an individual who may be escalating.

Body Language

Instead Of:	Try…
Standing rigidly directly in front of the person	Keeping a relaxed and alert stance off to the side of the person
Pointing your finger	Keeping your hands down, open, and visible at all times
Excessive gesturing or pacing	Using slow, deliberate movements
Faking a smile	Maintaining a neutral and attentive facial expression

Reporting

Reporting is critical. Threats that are not known cannot be managed.

- ✓ Establish organizational policy
- ✓ Ensure clear, simple and transparent procedures for reporting
- ✓ Develop and implement a confidential mechanism for tracking reported activities
- ✓ Coordinate with other stakeholders to manage reported threats

Ensure your personal safety before making a report

What to Report

When Calling 9-1-1:

If the person of concern is directly threatening you or others, if a weapon of any kind is involved, or you feel that the threat of violence is imminent, retreat and **call 9-1-1**

The 9-1-1 call taker will need specific information to provide an appropriate response

- Your name
- The location of the incident
- The location of the person of concern
- Your exact location
- A description of the situation
- Is the incident still in progress?
- A physical description of the person of concern
- The type and number of weapons, if any
- The number of potential victims

CISA Resources

ACTIVE SHOOTER PREPAREDNESS

Web presence with fact sheets, videos, translated materials:
cisa.gov/active-shooter-preparedness

- *Options for Consideration* video
- *Active Shooter Preparedness: Access and Functional Needs: What You Should Know* video
- Online course: IS-907 *Active Shooter: What You Can Do*
- *Emergency Action Plan Guide, Video, Template*

NON-CONFRONTATIONAL TECHNIQUES

- *Insider Threat Mitigation Guide*
  - cisa.gov/insider-threat-mitigation
- *Pathway to Violence* video
- *De-Escalation Series*
  - cisa.gov/de-escalation-series
- *Employee Vigilance Through the Power of Hello*
  - cisa.gov/employee-vigilance-power-hello
  - Translated in 18 languages

SECURING PUBLIC GATHERINGS

Business and critical infrastructure security resources:
cisa.gov/securing-public-gatherings

- *Physical Security Considerations for Temporary Facilities*
- *Personal Security Considerations*
- *Protecting Infrastructure During Public Demonstrations*
- *Protecting Patrons in Outdoor Eating Venues*
- *Protecting Patrons During the Holiday Shopping Season*
- *Vehicle Ramming Attack Mitigation*

SECURITY PLANNING RESOURCES

- CISA
  - Hometown Security Tools and Resources
    - cisa.gov/tools-and-resources
  - School Safety and Planning Resources
    - cisa.gov/school-safety-and-security
- FEMA – Planning Guides
  - fema.gov/emergency-managers/national-preparedness/plan
- DHS – Business Continuity Plans
  - ready.gov/business-continuity-plan

For more information:
www.cisa.gov

Questions?
Email:
CISARegion8trainingexercise@cisa.dhs.gov