ACTIVE ASSAILANT PREPAREDNESS AND SECURITY RESOURCES

Is There a Threat?

- There is no known specific threat to summer camps
- Recent and historical events suggest a general elevated threat
  - National Threat Advisory System Bulletin- lone offenders
  - Life stressors and grievances from economy, social isolation from COVID, etc.
  - Mass media coverage
- These incidents, while tragic, are *very* rare
- You can prepare for and prevent these events!

Awareness + Action = Prevention

Connect, Plan, Train, Report

- Connect- meet your 911 responders
  - Host a “First Responder Day” or just a walkthrough at camp
- Plan- a good plan now is better than a perfect plan later
  - Keep it simple and easy to learn and execute
  - Develop more detailed plans in the off-season
- Train- brief and rehearse your Emergency Action Plan with staff
  - This can be as simple as a staff “huddle” or a more structured, scripted event
  - Share your plan with your first responders
- Report- situational awareness is critical!
  - Establish a reporting process at camp
  - Encourage staff to “trust their gut”- if it *feels* wrong, it probably is

Response to an Active Assailant

- Pick a protocol that works for you
  - Run, Hide, Fight
  - Standard Response Protocol (“I Love You Guys” Foundation)
  - ALICE
- You are playing for *time*!
  - These incidents are typically short, but…
  - Rural camp locations may increase law enforcement response time

- Use your advantages- Camp structures, terrain, and vegetation provide cover and concealment
- Fight only if you must- but if you must, commit completely to it
  - Attacks normally end at first meaningful resistance
  - Swarm the attacker, use improvised weapons- anything to overwhelm, confuse, or disable the threat

Active Shooter Preparedness

CISA's Active Shooter Preparedness Program supports stakeholders in security capacity building against the active shooter threat—the most prominent attack method in the U.S.

cisa.gov/active-shooter-preparedness

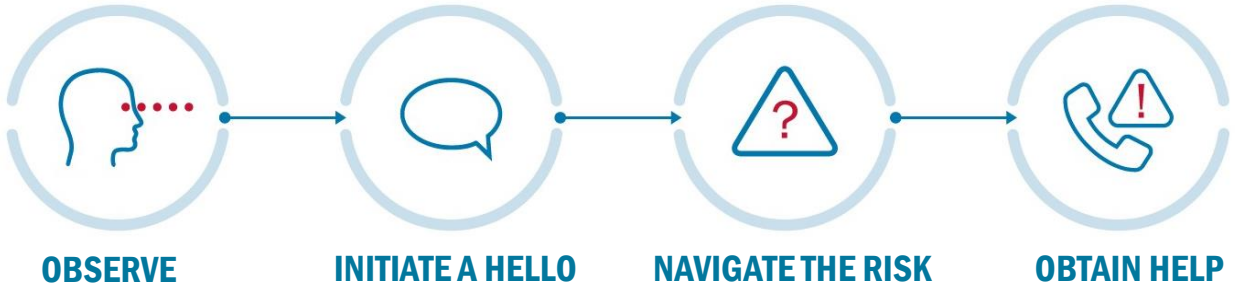
- **In-Person and Virtual Workshops**
- **Independent Study**
- **Active Shooter Mitigation Security Guidance**
- **Translated Materials**
- **Instructional and Informational Videos**
- **Outreach and Partnerships**

Employee Vigilance through the Power of Hello

Promotes employee vigilance

Alert personnel can spot suspicious activity and report it

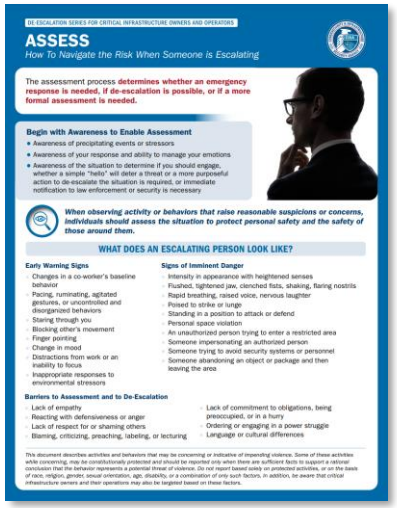
Used effectively, the right words can be a powerful tool



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.

cisa.gov/employee-vigilance-power-hello

De-Escalation Series



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

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 - Individuals are encouraged to use 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 - 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

Security Best Practices

Establish a multi-layered plan for security, identify clear roles and responsibilities

Conduct a vulnerability assessment to understand the risks specific to your location

Assess current doors, ensure they can withstand a determined intruder for up to ten minutes

Develop an emergency action plan - coordinate, train, and exercise the plan with local law enforcement and first responders

Outer, middle, and inner perimeter security considerations Lights, CCTV, windows, access control

A welcoming environment does not mean a defenseless one.

cisa.gov/hometown-security
cisa.gov/securing-public-gatherings
cisa.gov/cisa-tabletop-exercises-packages

Protecting K-12 Schools

Federal School Safety Clearing House

The **CISA School Safety Task Force** manages and administers the Federal School Safety Clearinghouse, an interagency effort between the Departments of Homeland Security, Justice, Education, and Health & Human Services to **coordinate Federal efforts on school safety and security**

- Provide one-stop access to school safety resources and programs through SchoolSafety.gov
- Connect school safety stakeholders at Federal, state, local, tribal and territorial levels
- Dynamic and multi-pronged approach to unique needs of schools
- Identify gaps in knowledge, resources, technologies and recommend best practices
- Increase awareness and coordination of school safety mission and resources
- Identify actionable steps schools can take to bolster safety across the preparedness continuum

schoolsafety.gov

CISA K-12 School Security Guide and Survey

Provide schools with a comprehensive **doctrine and systems-based methodology** for vulnerability assessment, planning and implementation of layered security elements.

Associated Product Suite

- CISA K-12 School Security Guide (3rd Edition)
- School Survey (Assessment Tool)
- Vulnerability Assessment Tool Training
- Systems-Based Methodology Training
- Train-the-Trainer Toolkit

Mitigating Attacks on Houses of Worship Security Guide

CISA **analyzed ten years of targeted attacks** on houses of worship between 2009 and 2019

Take a **holistic approach to security** by assigning clear roles and responsibilities and creating a multi-layered security plan

A robust security plan should be **tailored to the specific needs and priorities** of the house of worship

Conduct a **vulnerability assessment to understand the risks to the house of worship** from which you may prioritize implementing any subsequent safety measures.

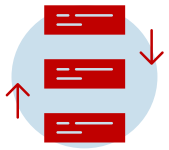
cisa.gov/mitigating-attacks-houses-worship-security-guide

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

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

For more information:
cisa.gov/securing-public-gatherings

To reach a Protective Security Advisor:
cisa.gov/protective-security-advisors
central@cisa.dhs.gov

Questions?
CISA.ISD.OSP_Active_Assailant_Security@cisa.dhs.gov