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
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.

[Diagram showing CISA Active Shooter Preparedness with icons for In-Person and Virtual Workshops, Independent Study, Active Shooter Mitigation Security Guidance, Instructional and Informational Videos, Translated Materials, Outreach and Partnerships.]
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](https://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

June 20, 2022
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
Federal School Safety Clearing House


**Federal School Safety Clearing House**

- 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

**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**

- School Survey (Assessment Tool)
- Vulnerability Assessment Tool Training
- Systems-Based Methodology Training
- Train-the-Trainer Toolkit

*schoolsafety.gov*
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.

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

[1]. Does the house of worship have a security manager or committee to make security management decisions?

<table>
<thead>
<tr>
<th>QUESTION</th>
<th>VERY LOW</th>
<th>LOW</th>
<th>MEDIUM</th>
<th>HIGH</th>
<th>VERY HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Does the house of worship have a security manager or committee?</td>
<td>Yes</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[2]. 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.

[3]. The house of worship has a security manager or committee. Security management activities are regularly scheduled but not coordinated with other committees, departments, and groups, but additional personnel are needed to support the facility’s security mission.

[4]. The house of worship has a security manager or committee. Security management activities are not regularly scheduled or coordinated with other committees, departments, and groups.

[5]. The house of worship does not have a security manager or committee.

[cisa.gov/houses-of-worship]
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