



INSTRUCTIONAL GUIDE

TO THE CISA ACTIVE ASSAILANT EMERGENCY ACTION PLAN TEMPLATE

FEBRUARY 2025

TABLE OF CONTENTS

OVERVIEW OF INSTRUCTIONAL GUIDE	3
1. APPLICABILITY AND SCOPE	4
Developing the Applicability and Scope Section of Your EAP.....	4
2. KEY ROLES AND RESPONSIBILITIES	5
3. FLOOR PLANS AND MAPS	9
4. FACILITY EMERGENCY ACCESS PREPAREDNESS	12
5. EMERGENCY COMMUNICATIONS	13
Emergency Response Notification.....	13
Internal Alert Notification Procedures.....	16
External Alert Notification Procedures.....	16
Public Information Coordination and Dissemination.....	17
6. PROCEDURES FOR EVACUATION, LOCKDOWN, AND SHELTER-IN-PLACE	19
Evacuation Procedures.....	19
Lockdown/Shelter-in-Place Procedures.....	20
7. RESPONSE PROCEDURES DURING AN ACTIVE ASSAILANT INCIDENT	23
Individual Response Procedures.....	23
When Law Enforcement Arrives.....	24
8. ACCOUNTABILITY	26
Personnel and Procedures.....	26
9. RECOVERY	28
Recovery Planning.....	28
Community Resources.....	28
Short-Term Recovery.....	29
Mid- to Long-Term Recovery.....	29
Business Continuity.....	30
10. TRAINING AND EXERCISES	31
Individuals Responsible for Training.....	31
Training.....	31
Exercises.....	32
RESOURCES	34

OVERVIEW OF INSTRUCTIONAL GUIDE to the CISA Active Assailant Emergency Action Plan Template

The Cybersecurity and Infrastructure Security Agency (CISA) developed the Active Assailant Emergency Action Plan (EAP) Template and this corresponding Instructional Guide to help critical infrastructure organizations and venues develop a comprehensive and implementable EAP. This resource provides guidance to assist users with completing each section of [CISA's EAP Template](#), and includes examples and additional resources for developing an effective plan.

An EAP outlines response procedures and actions for organizations and their personnel during emergency situations. Organizations should develop and implement EAPs to safeguard people, property, and systems against serious injury, loss of life, damage to property, or compromise resulting from active assailant threats.

CISA defines “active assailant(s)” as:

one or more individuals actively engaged in killing or attempting to kill people in a populated area.¹

Active assailant incidents impact all areas of society, including where we work, learn, play, shop, and worship. These incidents come at a high cost, not only in terms of casualties and injuries, but also in the form of long-term economic, social, and emotional impacts for communities, organizations, and individuals. An active assailant attack could involve, but is not limited to, the following weapons: firearms, edged weapons, vehicles, incendiary devices, explosives, and/or chemicals. Planning considerations for certain active assailant incidents can be found in [Section 7](#) of this guide.

DISCLAIMER: The Active Assailant Emergency Action Plan Template and this Guide to the Template were created by the Cybersecurity and Infrastructure Security Agency (CISA) for the purpose of mitigating the threat posed by Active Assailant incidents. The recommendations, approaches, techniques, and tactics described in this document are offered as options for consideration. They are not intended to mandate policy or direct any action. CISA accepts no liability for the failure of this guidance to prevent an active assailant incident.

¹ CISA, Physical Security Performance Goals for Faith-Based Communities, [cisa.gov/resources-tools/resources/physical-security-performance-goals-faith-based-communities](https://www.cisa.gov/resources-tools/resources/physical-security-performance-goals-faith-based-communities)

1. APPLICABILITY AND SCOPE

Developing an EAP can help organizations prepare for, respond to, and recover from an active assailant incident. Key personnel should be familiar with, trained on, and able to quickly access the EAP during an incident. The EAP should account for all individuals in an organization, including those with access and functional needs. It should supplement the organization's All Threats/Hazards Facility Security Plan. Organizations should consider implementing security policies and plans that assign responsibilities and establish procedures to protect people and assets.

Developing the Applicability and Scope Section of Your EAP

Applicability

The EAP applies to all specified organizational facilities and should align with the organization's All Threats/Hazards Facility Security Plan. Separate EAPs may be needed for primary and off-site locations, focusing on the unique characteristics of each site or facility.

Scope

An EAP provides detailed procedures, structure, and guidance for personnel when preparing for, responding to, and recovering from an active assailant incident. Personnel should be trained on their individual roles and responsibilities before an incident occurs to increase survivability and enhance resilience.

Organizations should review the EAP annually and update it based on evolving threats, incidents, resources, updated policies, facilities, or equipment, as well as feedback from exercises.

i EXAMPLE — Applicability and Scope Section:

Overview of our EAP:

Our organization's EAP provides a structured plan to help personnel respond effectively during an active assailant incident. The primary goal of the EAP is to enhance survivability and reduce the impacts of an incident. This EAP identifies team member training and response protocols, as well as security procedures to ensure the organization and business complex can effectively prevent and respond to an active assailant incident.

Our organization's EAP applies to buildings A, B, and C within the business complex and aligns to our overarching security plan. This EAP was last reviewed and updated on October 15, 2023.

2. KEY ROLES AND RESPONSIBILITIES



When developing an EAP, organizations should establish a collaborative Emergency Action Planning Team that will develop the organization's EAP and implement recommended security practices. This team should be diverse and include representatives from across the organization, including those with access and functional needs, first responders, and individuals involved in emergency management. While there is no set number of people required for an Emergency Action Planning Team, a larger team can provide varied experiences and inputs to enhance security. It is critical to appoint one individual as the team leader responsible for timelines, accountability, and coordination with organizational management for input and approval.

When assembling an Emergency Action Planning Team, organizations should consider including individuals both internal and external to the organization, which may include:

Internal Partners to Consult		
Senior Executive	Crisis/Incident/ Emergency Manager	Facility/Maintenance Manager
Security Director/Manager	Operations Manager	Information Technology
Individuals with disabilities and access and functional needs	Finance	Legal Advisor
Communication Manager or Public Information Officer (PIO)	Human Resources	Safety Staff
External Partners to Consult		
Law Enforcement	Fire Department	Emergency Medical Services
CISA Protective Security Advisor (PSA)	Neighboring Facilities	Tenants
Vendors	Insurance Representative	Healthcare and Public Health
Faith-Based Organizations	State or Regional Fusion Centers	Social Services

Crisis/Incident/Emergency Manager

The Crisis/Incident/Emergency Manager typically leads the Emergency Action Planning Team, overseeing security-related matters. Ideally, this person is a full- or part-time staff member or engaged volunteer. Larger organizations may have a designated Emergency Manager responsible for these functions.

Emergency Action Planning Team

The Emergency Action Planning Team supports the Crisis/Incident/Emergency Manager by conducting research, assessing needs, providing recommendations, and developing the EAP. Team members should possess a range of skills, such as knowledge and experience in security, law enforcement, facility management, mental health, emergency preparedness, incident management, public relations, and insurance, among others. Other valuable skill sets could include policy development, strategic planning, finance and accounting, and training.



Roles and Responsibilities

A comprehensive EAP outlines key roles and responsibilities for all relevant personnel in the event of an incident and should be tailored to the organization's size, culture, needs, mission, and resources. The examples provided in the following table identify suggested roles and responsibilities for designated individuals on the Emergency Action Planning Team. Depending on the organization, the individuals in these roles may perform some, but not all, of the sample responsibilities outlined below.

i EXAMPLE — Roles and Responsibilities Section:

Title/Role	Responsibilities/Duties
<p>Crisis/Incident/Emergency Manager (Business/Government Facilities)</p>	<ul style="list-style-type: none"> • Develop and implement active assailant security policies and practices and evaluate their effectiveness. • Oversee EAP development. • Lead response operations throughout an active assailant incident.
<p>Site Director (Business/Government Facilities)</p>	<ul style="list-style-type: none"> • Initiate lockdown, evacuation, or shelter-in-place procedures. • Activate internal notification protocols and communicate with staff using handheld radios, public notification systems, automated phone/text messages, etc. • Activate external notification protocols, inform off-site personnel, the surrounding community, and stakeholders via automated messaging. • Provide support to office manager and security manager, if necessary, in communicating with 9-1-1 dispatcher. • Work with maintenance manager to facilitate first responder site/building access. • Assist with EAP development.
<p>Security Director/Manager (Business/Educational/ Government Facilities)</p>	<ul style="list-style-type: none"> • Direct security operations for all aspects of the organization's safety and security. • Support site director in implementing lockdown and evacuation protocols. • Assist first responders as needed. • Secure all internal stairwell entry doors. • Aid in evacuating and directing personnel to designated safe areas. • Assist with EAP development.
<p>Safety Manager (Business/Educational/ Government Facilities)</p>	<ul style="list-style-type: none"> • Conduct safety meetings. • Design, implement, and monitor safety protocols. • Ensure organization complies with safety standards and regulations. • Liaise with external agencies. • Ensure safety of staff and visitors. • Assist with EAP development.
<p>Principal (Educational Facilities)</p>	<ul style="list-style-type: none"> • Activate lockdown, evacuation, or shelter-in-place procedures. • Communicate with staff via handheld radios and intercom system. • Trigger external notification protocols, which could include informing parents, the surrounding community, and stakeholders through automated email/text/phone/social media messages. • Supply law enforcement with facility emergency access kit. • Collaborate closely with first responders. • Assist with EAP development.


i **EXAMPLE – Roles and Responsibilities Section:**

Title/Role	Responsibilities/Duties
Facility/Maintenance Manager (Business/Educational/ Government Facilities)	<ul style="list-style-type: none"> • Support site security. • Assist in evacuating organizational personnel. • Provide support to first responders for building-related questions or issues. • Support security manager with 9-1-1 notification and subsequent emergency announcements. • Coordinate with and assist first responders throughout all incident phases. • Oversee building repairs following an incident. • Assemble facility emergency access kit. • Assist with EAP development.
Human Resources (Business/Government Facilities)	<ul style="list-style-type: none"> • Conduct employee screening and background checks. • Create a system for reporting potentially violent behavior. • Make counseling services available to employees. • Regularly update contact information and personnel rosters. • Assist with EAP development.
Communications Manager/ Public Information Officer (PIO) (Business/Government Facilities)	<ul style="list-style-type: none"> • Manage internal and external communication during emergencies. • Coordinate with emergency services, stakeholders, and employees. • Provide and coordinate updates and instructions to staff, family, the public, and the media. • Assist with EAP development.
Access and Functional Needs (AFN) Advisor (Business/Educational/ Government Facilities)	<ul style="list-style-type: none"> • Support and assist the Crisis/Incident/Emergency Manager on matters related to individuals with disabilities and access and functional needs. • Ensure EAP(s), evacuation instructions, and other relevant information address the needs of individuals with access and functional needs. • Assist with EAP development.
Medical Team/Nurse (Business/Educational/ Government Facilities)	<ul style="list-style-type: none"> • Assist with evacuation efforts. • Provide treatment to those injured at casualty collection and/or safe areas. • Collaborate with site director and security manager. • Assist first responder and EMS personnel if required. • Assist with EAP development.
Support Staff/Team Member (Business/Educational/ Government Facilities)	<ul style="list-style-type: none"> • Respond promptly to active assailant incident alert. • Assess and choose applicable response options (i.e., “Run-Hide-Fight”) based on the situation and organizational policy. • Call 9-1-1 when safe and provide necessary information. • Contact first line supervisor via phone, text message, or handheld radio to provide status updates. • Assist other team members if able and safe. • Assist with EAP development.



Facility Information and Access

Facility management personnel play a critical role in organizational safety and security, bringing detailed knowledge of an organization's building(s) and grounds. They can provide essential insights and answer questions from law enforcement and first responders arriving on the scene regarding site layout, entry/exit points, evacuation routes, optimal entry points for first responders, outer site/building access routes, and vehicle staging areas for emergency vehicles.

When identifying points of contact (POCs), consider the following:

- Develop and maintain contact information for facility management personnel and distribute to local first responder organizations.
- Identify multiple POCs to ensure adequate coverage in an emergency.
- Identify POCs who represent the site/building, maintenance, and security departments.

i EXAMPLE – Points of Contact for Facility Information and Access Section:

Title/Role	Name	Phone Number	Alternate Phone	E-mail
Site Director				
Maintenance Supervisor				
Security Director/ Manager				

To learn more about roles and responsibilities, review the following resources:

- CISA, Security Planning Workbook, [cisa.gov/resources-tools/resources/security-planning-workbook](https://www.cisa.gov/resources-tools/resources/security-planning-workbook)
- FEMA, Emergency Management – Planning Guides, [fema.gov/emergency-managers/national-preparedness/plan](https://www.fema.gov/emergency-managers/national-preparedness/plan)
- FEMA, National Incident Management System (NIMS), NIMS Components – Guidance and Tools, [fema.gov/emergency-managers/nims/components](https://www.fema.gov/emergency-managers/nims/components)

3. FLOOR PLANS AND MAPS















Organizations should include facility floor plans and maps in the EAP to help personnel and first responders navigate, evacuate, and respond quickly and accurately during an active assailant incident. These plans and maps should identify entry/exit points, assembly points, emergency access points, and locations for key equipment (e.g., fire extinguishers and first-aid kits/automated external defibrillators [AEDs]), coordinating with local law enforcement for accuracy.

Facility floor plans and overview maps help familiarize personnel and first responders with key aspects of an organization’s building(s) and grounds, including the surrounding area, facilitating a faster and safer response during an incident.

When developing floor plans, consider the following:

- Ensure floor plans provide basic information for emergency response, evacuation, and communication procedures with on-site personnel.
- Identify and highlight primary and alternate exit points. Exits should be clearly marked, well lit, unobstructed, and as far away from each other as possible to minimize the possibility that both may become blocked in an emergency.
- Identify location(s) of first-aid kits, which could include AEDs and severe bleeding kits, and facility emergency access kits.

When creating maps, consider the following:		
 Buildings	 Facility/Campus Entry and Exit Points	 Parking Lots
 Playgrounds	 Loading Docks	 Gates/Fences
 Vehicle/Pedestrian Entry Points	 Surrounding Businesses and Residential Neighborhoods	 Adjacent Streets
 Areas of Concern*	 Safety, Staging, and Medical Triage Areas	 Evacuation Routes for Personnel

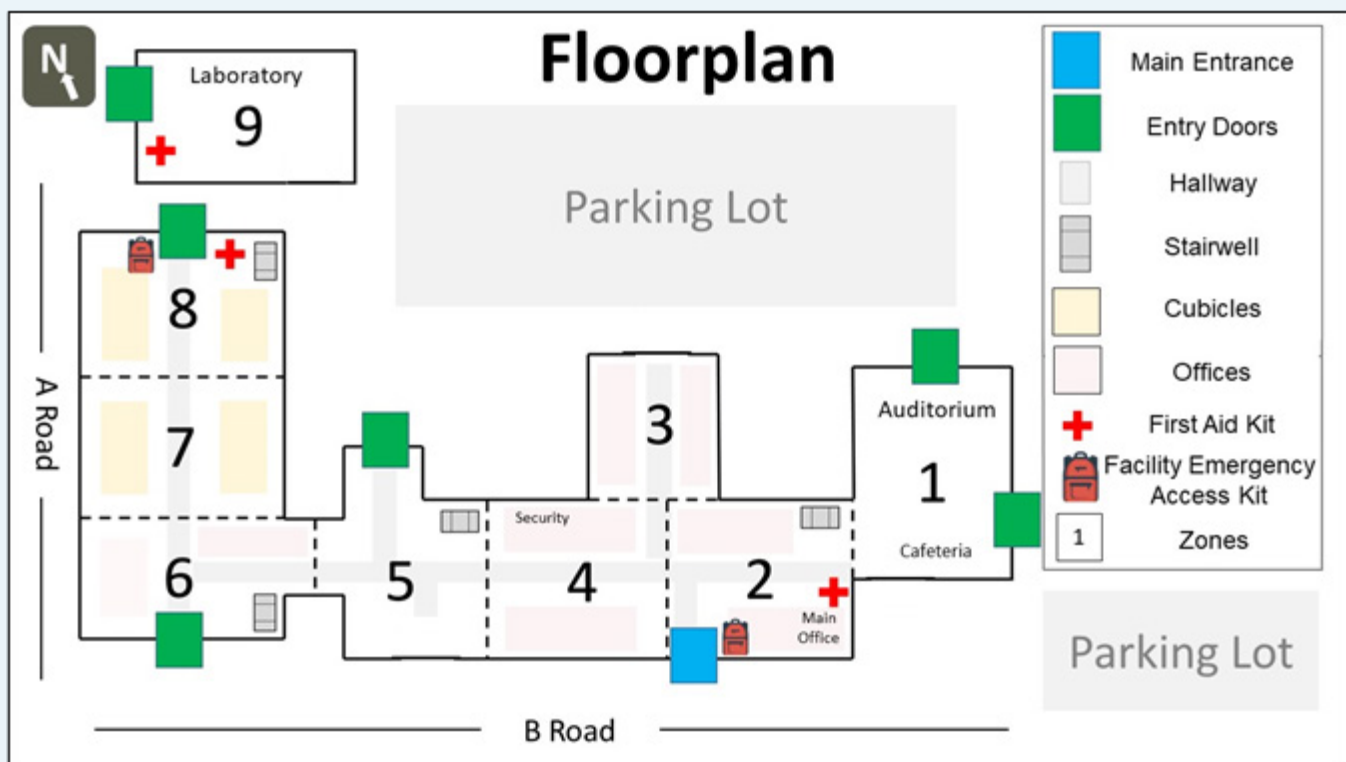
*i.e., spaces or areas where large groups of people gather, areas law enforcement may have difficulty accessing, or outside areas that may present security concerns.



EXAMPLE – Floor Plans and Maps Section:

Our organization’s floor plan is divided into a strategically planned zone grid to help first responders quickly locate an active assailant or other threat and help personnel safely navigate the Headquarters (HQ) building. The purpose of this zone grid is to provide first responders with a simple approach to reach the threat or incident quickly. The zone grid is divided into the following areas:

1. Spaces of Interest (e.g., offices, cubicle spaces, storage rooms)
2. Entry/Exit Points
3. Facility Emergency Access Kit





i EXAMPLE – Floor Plans and Maps Section:

The area map of the HQ business complex provides an aerial view of the building and highlights the physical structure(s), all usable entry/exit points (to include vehicle entry/exit points), working spaces (e.g., parking lots, loading docks), adjacent streets/roadways, and surrounding businesses/residential neighborhoods. The site perimeter is marked by a combination chain-link/wrought iron/wood fence line. The site’s north, east, and south sides are surrounded by businesses, and the west side borders a residential neighborhood. Two high-traffic roads run parallel to the site, and both can be used for site entry. Employees/visitors access the site using two gated vehicle entry points, which can support first responder vehicles. During working hours (7:00am – 5:30pm) these gates are open.

The Overview Map is divided into the following areas:

1. HQ Building
2. Evacuation Routes
3. Danger Areas
4. Safe Areas/Casualty Collection Points



- Evacuation Route
- Danger Areas
- Safe Area
- Main Entrance
- Entry/Exit Doors
- Facility Emergency Access Point

Evacuation Routes can offer a level of cover and concealment for evacuating personnel from directed gunfire coming from the building.

Danger Areas offer minimal cover and concealment from directed gunfire for evacuating personnel.

Safe Areas are positioned at various points that offer a basic level of cover and concealment at a safe distance from the building.

Everyone must make an individual determination on which exits, evacuation routes, and safe areas to use based on circumstances and proximity to the assailant(s).

Floor plans and maps should be added to the Appendix Section of the EAP.

To learn more about floor plans and maps, review the following resources:

- CISA, Infrastructure Visualization Platform, cisa.gov/resources-tools/services/infrastructure-visualization-platform-ivp
- FBI, Developing Emergency Operations Plans: A Guide for Businesses, fbi.gov/file-repository/active-shooter-guide-for-businesses-march-2018.pdf/view
- OSHA, Emergency Action Plan: Evacuation Elements, osha.gov/etools/evacuation-plans-procedures/eap/elements

4. FACILITY EMERGENCY ACCESS PREPAREDNESS

First responders and law enforcement may be unfamiliar with a facility's layout, which may hinder incident response efforts. Site visits can help familiarize them with the facility, key personnel and provide an opportunity for them to advise on response procedures. Creating a facility emergency access kit can help expedite first responder facility access and navigation during an emergency incident.

When assessing facility emergency access preparedness, consider the following:

- Identify special equipment necessary to assist those with special needs, as required.
- Invite local law enforcement and other first responders to participate in annual facility visits.
- Conduct tours to familiarize first responders with the site layout.
- Provide first responders with information that includes facility floor plans, entry/exit access points, etc.
- Determine where to place facility emergency access kit(s) and how law enforcement will access them.
- Identify contents for facility emergency access kit(s).

When assembling facility emergency access kit(s), consider including:

- Clearly labeled and laminated floor plans and overview maps.
- Laminated contact information for POCs.
- Labeled key/access card(s) for internal/external doors with a lanyard.
- Elevator keys (if applicable).
- Two-way radios with extra batteries.

Facility emergency access kits should contain the most recent floor plans and maps and be periodically updated. If feasible, include multiple sets of items for first responder teams.

***i* EXAMPLE — Facility Emergency Access Preparedness Section:**

The purpose of facility emergency access preparedness is to ensure first responders can independently navigate our facility without assistance from building or organizational personnel. Our main building has two facility emergency access kits located outside the main entrance door and at the rear loading dock (see floor plans located in Appendix A of our EAP).

Each facility emergency access kit includes the following:

1. (4) Floor plan and area maps
2. (4) Site/building POC lists
3. (4) Key/card(s) for external doors
4. (4) Key/card(s) internal doors

To learn more about facility emergency access preparedness, review the following resources:

- CISA, Crisis Event Response and Recovery Access (CERRA) Framework, [cisa.gov/sites/default/files/2023-12/crisis-event-response-and-recovery-access-framework_112023_508.pdf](https://www.cisa.gov/sites/default/files/2023-12/crisis-event-response-and-recovery-access-framework_112023_508.pdf)
- FEMA, Emergency Management – Planning Guides, [fema.gov/emergency-managers/national-preparedness/plan](https://www.fema.gov/emergency-managers/national-preparedness/plan)
- OSHA, Emergency Preparedness and Response: Getting Started, [osha.gov/emergency-preparedness/getting-started](https://www.osha.gov/emergency-preparedness/getting-started)



5. EMERGENCY COMMUNICATIONS

In the event of an active assailant incident, organizations must be prepared to provide timely, accurate, and effective direction and information to impacted personnel; provide clear, real-time situational information to first responders; and inform the public as appropriate. EAPs should address both internal and external communications, outlining specific roles for responders.

When planning emergency communications, consider the following:

- Develop procedures for initial emergency notifications.
- Establish protocols for how to communicate updates to personnel and relevant stakeholders.
- Provide guidance for public information dissemination.

Emergency Response Notification

In an emergency, every member of an organization is responsible for contacting 9-1-1 as soon as they become aware of the incident and when it is safe to do so. Organizations should ensure personnel know how to report accurate and helpful information about an incident to 9-1-1 and should emphasize the importance of remaining calm, speaking clearly, and providing concise information.

Information relayed to dispatchers should be clear and concise, for example:

Caller: This is John Doe, I am at the XXX building, 123 W. First Street. We have an active assailant incident in progress. I saw two shooters with semiautomatic rifles on the second floor headed toward conference room A. They were both wearing black tactical pants. One had on a long black shirt, the other had a long black and white striped shirt, and both were wearing bulletproof vests. I am on the second floor, in room 207b. I have locked and barricaded the door and there are three other employees with me.

Dispatcher: Thank you, John. Keep your door locked and barricaded, and turn all phones to silent.

When developing emergency response notification procedures, consider the following:

 <p>Designate authorized personnel for initiating and updating notifications</p>	 <p>Assign individuals to be responsible for communicating with the media/public/external entities</p>	 <p>Develop pre-scripted messages to facilitate more effective communication during an emergency</p>
 <p>Establish information centers</p>	 <p>Develop guidance for managing rumors and disinformation*</p>	 <p>Implement multiple redundant mass notification mechanisms**</p>

*(e.g., monitoring AM/FM radio, social media, and television broadcasts), and correct misinformation promptly, if possible.

** (e.g., public announcement (PA) systems, handheld radios, audible/visual alarms, social media, and/or communication applications) and resilient procedures to ensure communications capability throughout an emergency.



Points of Contact Responsible for Communications

During an active assailant incident, organizations must be able to quickly identify who to contact. Once 9-1-1 has been notified, there may be a need to alert additional individuals within the organization, such as senior leadership or security staff.

When identifying POCs responsible for communications, consider the following:

- Designate a primary POC responsible for managing communication with emergency responders and on-site/off-site personnel, as well as tracking injured or missing personnel.
- Identify support/alternate personnel capable of assuming responsibilities if the primary POC is unavailable.
- Designate personnel from different buildings for internal and external communication to staff, first responders, the media, and community leaders, among others. This applies most often to larger organizations with multiple sites.
- Ensure all designated and support personnel are trained and familiar with their assigned roles and responsibilities.

i EXAMPLE — Points of Contact Responsible for Communications Section:

Our organization's designated personnel manage internal alerts, external communications, and notification processes during an active assailant incident or emergency. The primary person responsible for external communication will be the site supervisor. In the event the site supervisor is not available or is incapacitated, the front office manager or security supervisor will be responsible for emergency communications and notifications.

Listed below are the POCs responsible for communication and notification:

	Title/Role	Name	Phone Number	Alternate Phone	E-mail
P	Site Director	John Doe	555-555-5555	123-444-5555	jdoe@orga.com
A	Maintenance Supervisor	Jane Doe	555-555-5555	123-444-5555	jdoe@orga.com
A	Security Supervisor	Doe John	555-555-5555	123-444-5555	djohn@orga.com

When completing this section, note that "P" indicates a primary POC, and "A" indicates an alternate POC.



Issuing Active Assailant Incident Alert(s)

Organizations should ensure they have multiple communication mechanisms for issuing internal and external alerts before, during, and after an incident. Factors such as organizational purpose, structure, budget, resources, and site layout may determine the choice of systems, applications, and methods used to issue an alert.

When determining alert methods for active assailant incidents, consider the following:

- Identify communication systems for delivering emergency messages to on-site and off-site personnel, vendors, neighboring businesses, and community members.
- Establish processes and procedures for notifying individuals with sensory, intellectual, or cognitive disabilities; limited English proficiency; and others with access and functional needs.
- Ensure designated staff are trained to operate mass notification systems.

i EXAMPLE – Methods to Issue an Active Assailant Alert Section:

Our organization uses a multi-layered notification process to alert personnel of an active assailant incident and communicate internally with staff. We employ the following notification systems:

- **Building PA System:** The security office has overall authority and control to initiate a site-wide alert and lockdown in the event of an active assailant incident. The initial building alert will be issued over the PA system in the form of a verbal message and audible alarm blast.
- **Desk Phone Intercoms:** Each desk phone has an intercom feature with the capability to alert staff to a site-wide active assailant incident. This feature allows any staff member to issue an alert based on their direct knowledge of and proximity to an incident.
- **Handheld Radios:** Designated personnel in various sections can use handheld radios to issue an alert of an active assailant incident directly to the security office. Each handheld radio will be set to emergency channel. No communication will be conducted on this channel unless an active assailant incident notification is initiated.
- **Audible/Visual Alarms:** As an active assailant incident notification is issued, the PA system combined with the building's red lights will be used to alert deaf or hard-of-hearing personnel.

All personnel have the capability and responsibility to issue an alert for an active assailant incident. The system for issuing initial alerts is based on location and capability. To ensure complete and rapid notification, the preferred alert method is the building PA system.



Internal Alert Notification Procedures

As part of an effective response strategy, organizations should establish procedures and mechanisms to alert and update all stakeholders, including on-site visitors, during an active assailant incident. When determining alert notification methods, consider factors such as organizational size, number and type of personnel, visitors, and available resources.

When developing internal alert procedures, consider the following:

- Identify key personnel and their role in initiating on-site communications during an active assailant incident.
- Develop clear and concise pre-scripted alert messages to minimize response time.
- Ensure designated notification personnel receive regular training on the use of available and preferred communication tools.
- Ensure all personnel can receive alerts, both on site and off site, which could include vibrating alerts or tactile devices for individuals with access and functional needs.
- Identify and describe how to manage rumors and disinformation (e.g., monitoring AM/FM radio, social media, and television broadcasts) and correct misinformation as soon as possible.

i EXAMPLE – Internal Alert Notification Procedures Section:

Our organization's internal alert notification procedures start with our alert notification team, which has the primary responsibility of initiating a site-wide active assailant incident alert. Our alert notification team and personnel will use the following communication tools to alert personnel and visitors of an incident:

- The primary alert notification will be conducted over the PA system and with the Emergency Lighting System, which reaches every building within the business complex. These alerts will consist of an audible message in English and Spanish, followed by an alarm blast and a flashing red light signal.
- Immediately following the PA and Emergency Lighting System alerts, an alert will be sent via cell phone messaging and an automated call application that will provide details and directions in English and Spanish.
- Organizational personnel will use their voice, cell phone, email, software-based push notifications, or handheld radios to initiate the alert process.

External Alert Notification Procedures

Organizations should have established mechanisms and procedures to alert all off-site personnel, family members, other organizational members (e.g., headquarters, annex sites), vendors, contractors, the media, and neighboring businesses of an active assailant incident, instructing them to stay away from the site. Public messaging coordination may be required for larger organizations, involving internal teams and approval processes. Local law enforcement will likely be involved in external notification efforts and require the use of community resources.

POLICIES



When developing external incident alert procedures, consider the following:

- Coordinate with local law enforcement and emergency operations managers before establishing external alert procedures.
- Designate individuals responsible for sending external alerts.
- Choose communication tools for alerting external personnel of an incident (e.g., cell phone message, call app, or e-mail blast).
- Develop clear and concise pre-scripted messages for various incidents such as:
 - “Active assailant incident onsite. Stay away from location.”
 - “Active assailant incident in the area. Site is sheltering in place. Stay away from location.”
- Provide relevant follow-up notifications using chosen communications tools.

***i* EXAMPLE – External Alert Notification Procedures Section:**

The organization’s external notification procedure for an active assailant incident will be initiated by members of the alert notification team and sent through our emergency alert notification application via phone call or text message. External parties associated with the organization include off-site staff members, families, the HQ staff, neighboring facilities, community members, and law enforcement.

The organization’s external alert notification procedure is as follows:

1. Following an internal incident notification, designated alert notification team members will initiate cell phone messaging and calls to notify all parties and provide appropriate instructions and relevant information. Messages and calls should state, “Warning, ACTIVE ASSAILANT INCIDENT occurring at the organization’s main building. Stay away from area. Additional notifications to follow with updated information.”
2. A designated alert notification team member will trigger the external PA system to alert personnel and visitors in the parking lot and loading dock areas of the incident.
3. Designated personnel will provide hourly updates via cell phone messaging and mobile phone application following initial notification.

Public Information Coordination and Dissemination

Effective public communication before, during, and after an incident is crucial for protecting people and property, as well as maintaining credibility and public trust. Organizations should appoint a primary Public Information Officer (PIO) to engage with the public, the media, and the private sector. Larger organizations may designate additional spokespersons, with one serving as the primary. PIOs are responsible for developing and releasing incident-related information to the media, the public, and other agencies. Organizations should also consider creating a media and public engagement strategy to assist with public information coordination and dissemination.

PROCEDURE



When developing a media/public engagement strategy, consider the following:

- Develop pre-scripted messages or templates for active assailant incidents.
- Coordinate with key individuals for message clarity and consistency.
- Ensure accuracy of disseminated information.
- Manage rumors and misinformation during and after an incident.
- Use multiple communication channels to disseminate information (e.g., social media, text, website, email).
- Coordinate communication with local leaders and law enforcement.

Message Examples:

Initial Incident Message: “There is an ongoing active assailant incident occurring now at xxx Main Street in xxxx.

We are advising all people to stay away from this site until further notice.

Updated information will be provided to staff, family members, and the local community as available on our social media channels located here.”

Follow-Up Incident Message: “At 10:00am today, an individual entered our facility and proceeded to open fire on employees in the building. This is a mass casualty event and those injured have been taken to XXX hospital. The suspect was taken into custody by local law enforcement.

We are in communication with family members and the local community. We are currently providing support and will continue to do so in the coming days and weeks during this extremely difficult time. Currently, there is no longer a threat to those inside the facility or to anyone in the surrounding area.

Our organization executed our security protocols to ensure the security of our employees and local community. The safety of our community remains our top priority.”

To learn more about alerts and communications during an active assailant incident, review the following resources:

- CISA, Interagency Security Committee (ISC): Planning and Response to an Active Shooter Guide, [cisa.gov/resources-tools/resources/isc-planning-and-response-active-shooter-guide](https://www.cisa.gov/resources-tools/resources/isc-planning-and-response-active-shooter-guide)
- CISA, Priority Telecommunications Services, [cisa.gov/topics/emergency-communications/priority-services](https://www.cisa.gov/topics/emergency-communications/priority-services)
- CISA, Security Planning Workbook, [cisa.gov/resources-tools/resources/security-planning-workbook](https://www.cisa.gov/resources-tools/resources/security-planning-workbook)
- DHS, Ready.gov, Crisis Communications Plans, [ready.gov/business/emergency-plans/crisis-communications-plans](https://www.ready.gov/business/emergency-plans/crisis-communications-plans)
- FBI, Developing Emergency Operations Plans: A Guide for Businesses, [fbi.gov/file-repository/active-shooter-guide-for-businesses-march-2018.pdf/view](https://www.fbi.gov/file-repository/active-shooter-guide-for-businesses-march-2018.pdf/view)
- FEMA, Emergency Management - Comprehensive Preparedness Guide (CPG 101): Developing and Maintaining Emergency Operations Plans, September 2021, [fema.gov/emergency-managers/national-preparedness/plan#cpg](https://www.fema.gov/emergency-managers/national-preparedness/plan#cpg)
- FEMA, NIMS Implementation and Training: NIMS Basic Guidance for Public Information Officers, [fema.gov/emergency-managers/nims/implementation-training#guides](https://www.fema.gov/emergency-managers/nims/implementation-training#guides)
- FEMA, Preparedness Community - Active Shooter: Pay Attention to Emergency Notifications, community.fema.gov/ProtectiveActions/s/article/Active-Shooter-Pay-Attention-to-Emergency-Notification

6. PROCEDURES FOR EVACUATION, LOCKDOWN, AND SHELTER-IN-PLACE



In the event of an active assailant incident, personnel may need to evacuate a facility, lockdown, or shelter-in-place. To prepare for such an emergency, organizations should outline protocols in their EAP. Clear guidance during such incidents can save lives and reduce the risk of injuries. This section offers planning considerations and resources for developing organizational guidance and procedures for evacuation, lockdown, and shelter-in-place responses.

Points of Contact for Initiating Evacuation, Lockdown, or Shelter-in-Place

Organizational POC(s) responsible for decisions and notifications to initiate evacuation, lockdown, or shelter-in-place procedures should be identified in [Section 5, Emergency Communication](#).

Evacuation Procedures



EVACUATION is the organized and supervised withdrawal, dispersal, or removal of civilians from hazardous or potentially hazardous areas, and their reception and care in designated safe areas.²

Evacuation focuses on the courses of action organizations should execute when evacuating facilities, buildings, and grounds. Plans should cover all areas, including public, personnel-only, storage areas, and facility-adjacent spaces. All stakeholders should be familiar with evacuation routes.

Given the dynamic nature of active assailant incidents, evacuation strategies will differ from those for fires or natural disasters. During many active assailant incidents, mass evacuation may not be appropriate, and individuals may need to implement the **Run, Hide, Fight** model (or similar response protocols).

When developing evacuation planning procedures, consider the following:

- Identify conditions that would require evacuation.
- Designate individual(s) responsible for initiating evacuation protocols, in coordination with law enforcement.
- Communicate staging areas and designated locations for emergency response resources.
- Determine how to safely direct individuals to designated safe areas.
- Consider the possibility of a complex coordinated attack and that the safe area could be a secondary target for potential attacker(s).
- Identify methods for evacuating individuals with access and functional needs, including those with service animals, assistive devices, and language, transportation, or medical needs.
- Establish safe areas/rooms for individuals unable to evacuate.
- Identify primary and secondary evacuation routes with clear signs.
- Designate individuals responsible for maintaining personnel accountability.
- Review evacuation information, procedures, and responsibilities with organizational personnel.
- Conduct regular evacuation drills, both with and without first responders.

² DHS Lexicon, dhs.gov/publication/dhs-lexicon



i EXAMPLE – Evacuation Procedures Section:

Upon receiving an active assailant incident notification via the building's PA system and cell phone application, the building will immediately enter automatic lockdown. The organization's evacuation procedure during an active assailant incident relies on individual team members assessing their situations and determining whether evacuation is a safe and viable option.

If capable of evacuating and choosing to do so, personnel should observe the following guidelines:

1. Plan your exit route thoughtfully. Check your surroundings and avoid impulsive movements to avoid evacuating in the direction of the threat.
2. Anticipate multiple attackers.
3. Use the environment (e.g., cars, walls, trees) for cover and concealment.
4. Be alert to threats originating from inside the building.
5. Relocate to the furthest identified safe area or other safe location after evacuation.

Once at the safe area or other secure location:

1. Survey your surroundings for other potential dangers or attackers.
2. When it is safe to do so, contact your supervisor to provide accountability.
3. If security is compromised at the safe area, move to an alternate secure location.

Lockdown/Shelter-in-Place Procedures

During an active assailant incident, the organization may initiate **lockdown** or **shelter-in-place** procedures. Shelter-in-place focuses on remaining indoors, perhaps for an extended period, while lockdown focuses on securing the premises during an immediate threat. The primary objective of a lockdown is to ensure all people are secured quickly in areas away from immediate danger.



LOCKDOWN includes courses of action to ensure all persons are secured quickly in areas away from immediate danger.³



SHELTER-IN-PLACE includes taking emergency refuge within the nearest designated safe area until notification or determination that the situation has been resolved.⁴

³ FBI, Developing Emergency Operations Plans: A Guide for Businesses, [fbi.gov/file-repository/active-shooter-guide-for-businesses-march-2018.pdf/view](https://www.fbi.gov/file-repository/active-shooter-guide-for-businesses-march-2018.pdf/view)

⁴ DHS Lexicon, [dhs.gov/publication/dhs-lexicon](https://www.dhs.gov/publication/dhs-lexicon)



When developing lockdown and shelter-in-place procedures, consider the following:

- Identify threats requiring lockdown or shelter-in-place responses.
- Determine circumstances in which lockdown will be initiated.
- Determine circumstances in which shelter-in-place will be initiated.
- Identify physical spaces that can provide protection from an active assailant within the facility.
- Ensure functional locking mechanisms for all exits and entrances.
- Establish protocols for locking exterior, interior, and gate doors and access points.
- Secure exterior perimeter.
- Communicate lockdown or shelter-in-place directives, which should be able to be received by non-English speaking personnel, individuals with disabilities, and those with access and functional needs.
- Procedures should account for individuals who require regular administration of medication, who use medical equipment, or require personal assistance services.
- Designate and train key personnel responsible for initiating a lockdown or shelter-in-place.
- Develop procedures for accounting for staff, visitors, vendors, customers, etc.
- Coordinate with law enforcement or first responders to determine when lockdown or shelter-in-place procedures can conclude.

***i* EXAMPLE – Lockdown and Shelter-in-Place Procedures Section:**

The organization's emergency response team issues a lockdown or shelter-in-place alert based on the situation on-site or in the general area. If the site is directly targeted, the emergency response team will automatically initiate a lockdown order for the entire building that will lock all exterior doors. In the event of an incident in the immediate vicinity, a lockdown or shelter-in-place alert will be issued. The alert will go out over the PA system and via our cell phone application. In case of an extended lockdown or shelter-in-place, each office space is equipped with a red emergency supply bag containing food, water, blankets, batteries, flashlights, medical supplies, and bathroom necessities.

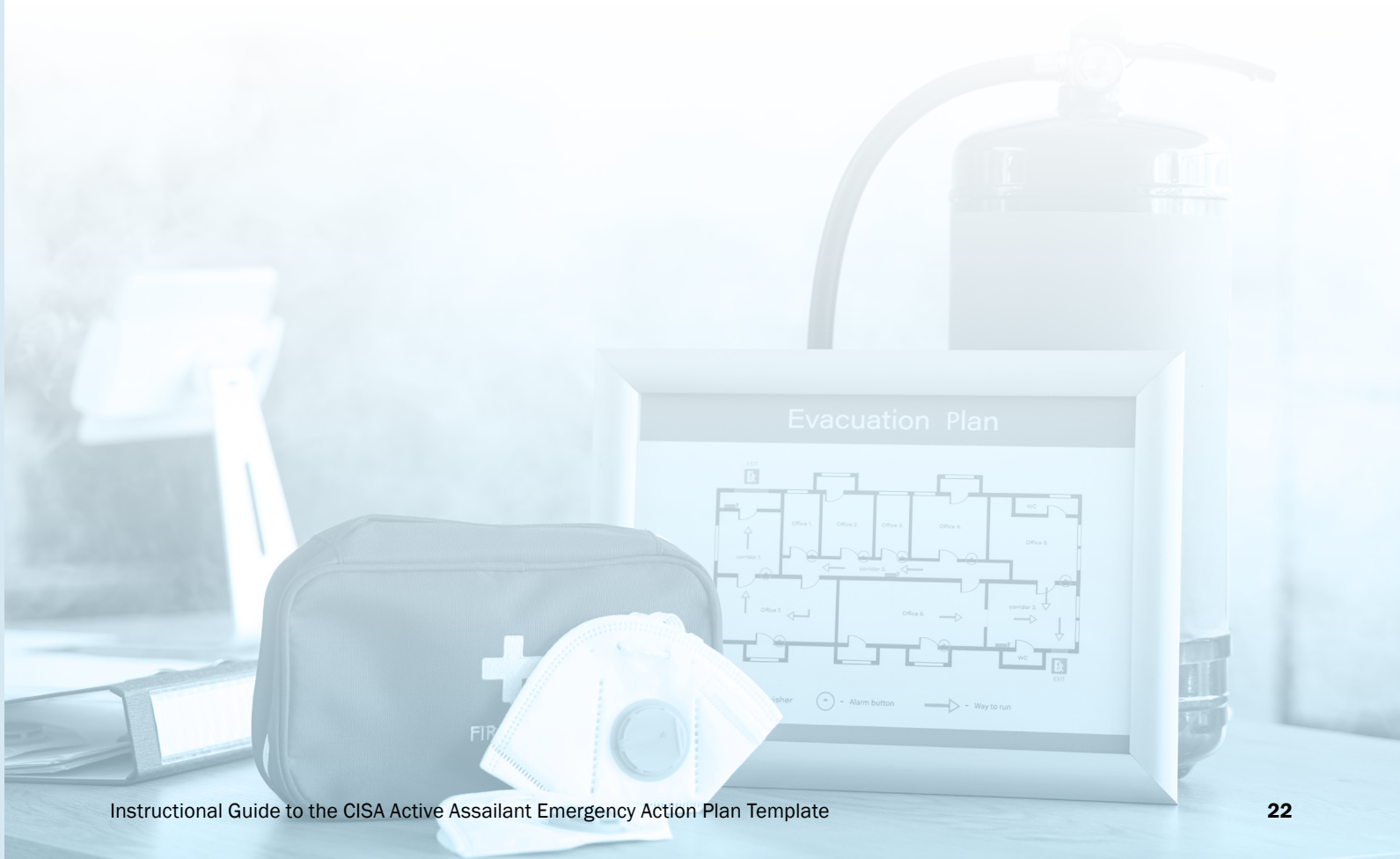
When a lockdown or shelter-in-place is initiated, employees should:

- Attempt to find a room with a door that has a lock or identified safe room.
- Lock, cover, and/or block door windows, glass door inserts, and other entry points.
- Turn off lights and cover automatic light sensors.
- Remain silent.
- Silence phones and electronics.
- Quietly block doors with heavy items.
- If possible, stay away from the door.
- If possible, seek cover and concealment.



To learn more about evacuation, lockdown, and shelter-in-place procedures, review the following resources:

- CISA, ISC, Occupant Emergency Programs Guide, cisa.gov/resources-tools/resources/isc-occupant-emergency-programs-guide
- FBI, Developing Emergency Operations Plans: A Guide for Businesses, fbi.gov/file-repository/active-shooter-guide-for-businesses-march-2018.pdf/view
- FEMA, Evacuation and Shelter-in-Place, “Planning Considerations: Evacuation and Shelter-in-Place,” fema.gov/emergency-managers/national-preparedness/plan/evacuation-shelter-in-place
- FEMA, IS-360: “Preparing for Mass Casualty Incidents: A Guide for Schools, Higher Education, and Houses of Worship,” emilms.fema.gov/is_0360/media/276.pdf
- OSHA, Emergency Preparedness and Response: Getting Started, osha.gov/emergency-preparedness/getting-started
- OSHA, Evacuation Plans and Procedures eTool, osha.gov/etools/evacuation-plans-procedures/eap/elements





7. RESPONSE PROCEDURES DURING AN ACTIVE ASSAILANT INCIDENT



Clearly documented response procedures can increase survivability and help personnel understand their roles, responsibilities, and courses of action during an active assailant incident. While training and response procedures are critical, individuals will also need to rely on their own judgment during an incident. There is no one-size-fits-all response approach for active assailant situations. An active assailant may plan an attack based on access to a specific weapon, target availability, or other considerations. As such, personnel should understand response options for various threats so they can act decisively and reduce their risk during an incident. It is also important to help personnel understand how first responders and law enforcement might respond during an active assailant incident.

When developing response procedures for an active assailant incident, consider the following:

 <p>Firearm or Edged Weapon Incidents:</p>	<ul style="list-style-type: none">■ Determine immediate notification capabilities, such as using gun/gunshot detection systems.■ Evaluate the facility's structure and floor plans, including lockable rooms, open cubicle spaces, large open areas, glass walls/windows, elevators/escalators, and facility entrances/exits, among others.■ Identify spaces or structures that can shield people from gunfire, such as rooms with concrete walls and bulletproof/bullet-resistant doors and windows.■ Assess medical response capabilities, such as first aid kit availability, trained medical staff, and first aid-trained personnel.
 <p>Vehicle as a Weapon Incidents:</p>	<ul style="list-style-type: none">■ Assess vulnerabilities and potential targets for vehicle attacks, such as outdoor events or gatherings, parking lots, playgrounds, or outdoor seating areas.■ Identify personnel roles and responsibilities.■ Identify and implement permanent or temporary methods to prevent or stop a vehicle attack, such as trees, concrete barriers, bollards, or balusters.

Individual Response Procedures

Once an active assailant incident is identified, personnel should follow established or recommended individual response procedures (e.g., Run-Hide-Fight, Avoid-Barricade-Confront, Avoid-Deny-Defend). Individuals should be trained to act based on the type of weapon involved and their proximity to the incident, while also considering their unique access and functional needs, if applicable. An organization's EAP should outline all recommended training and individual response options.

When developing individual response procedures, consider the following:

- Identify potential methods of attacks, such as firearms, knives, or vehicles.
- Determine response options and training mechanisms, such as Run-Hide-Fight or Avoid-Deny-Defend.
- Consider individuals with disabilities, those with access and functional needs, and individuals with limited English proficiency when establishing procedures.
- Identify personnel roles and responsibilities.
- Assess the size and complexity of the facility.



i EXAMPLE – Individual Response Procedures Section:

Once an incident alert has been issued, employees should respond in accordance with the organization's Run-Hide-Fight video-based training and security procedures. Individual team members should assess their unique situation and proximity to the assailant(s) and independently decide on a course of action based on training and organizational guidance and procedures. Law enforcement will respond, secure the building, and neutralize the threat. Medical personnel will treat the injured once the scene has been secured. First responders will follow and implement their response protocols.

Once alerted to an active assailant incident, personnel should:

1. Evacuate if possible. Maintain awareness around the risk of multiple assailants and/or secondary attacks.
2. Before moving, have a planned destination.
3. If unable to evacuate, hide or shelter in place. Remain silent, silence phones and other devices, and lock and barricade doors.
4. When safe and able, call or text 9-1-1.
5. Remain flexible and be prepared to adjust your position or actions as the incident evolves.
6. When safe and able, contact your supervisor or other organizational leaders to confirm your status.

When Law Enforcement Arrives

Understanding how law enforcement and emergency medical services (EMS) typically respond during an active assailant incident can enhance overall safety and response efficiency. Law enforcement and EMS will execute procedures to eliminate the threat, secure the site, evacuate personnel, and treat any injured. In some locations, tactical EMS teams may follow close behind first responders to begin evacuating and treating the wounded.

When developing procedures to prepare for the arrival of law enforcement, consider the following:

- Inform and train personnel on first responder roles and actions.
- Determine how law enforcement will access the site.
- Identify organizational personnel to assist first responders.
- Determine a method for providing continuous information to law enforcement during the incident.

i EXAMPLE – When Law Enforcement Arrives Section:

When law enforcement and first responders arrive on-site and enter the building, expect them to follow their own procedures to eliminate the threat. Until the threat is neutralized, police will not help or treat the wounded. Once law enforcement clears sections of the building, EMS will likely begin helping those injured.

The organization and on-site personnel will perform the following actions to assist law enforcement and first responders arriving at the scene:

1. Personnel will follow all commands from law enforcement and first responder personnel.
2. When safe and able, the maintenance director and security manager will meet with law enforcement to assist as needed.
3. The site director and office manager will continue to provide all relevant information gathered from internal communication to the 9-1-1 dispatcher.



To learn more about response procedures during an active assailant incident, review the following resources:

- CISA, Active Shooter Pocket Card, cisa.gov/resources-tools/resources/active-shooter-pocket-card
- CISA, ISC Planning and Response to an Active Shooter Guide, cisa.gov/resources-tools/resources/isc-planning-and-response-active-shooter-guide
- CISA, Options for Consideration Video, cisa.gov/resources-tools/resources/options-consideration-video
- CISA, Tabletop Exercise Packages (CTEPs), cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages
- CISA, Vehicle Ramming Action Guide, cisa.gov/resources-tools/resources/vehicle-ramming-action-guide
- CISA, Venue Guide for Security Considerations, cisa.gov/resources-tools/resources/venue-guide-security-considerations
- FEMA, Attacks in Crowded and Public Spaces, ready.gov/public-spaces
- FEMA, Evacuation and Shelter-in-Place, “Planning Considerations: Evacuation and Shelter-in-Place,” fema.gov/emergency-managers/national-preparedness/plan/evacuation-shelter-in-place
- FEMA, IS-360: “Preparing for Mass Casualty Incidents: A Guide for Schools, Higher Education, and Houses of Worship,” emilms.fema.gov/is_0360/media/276.pdf
- FEMA, Preparedness Community - Active Shooter: Pay Attention to Emergency Notifications, community.fema.gov/ProtectiveActions/s/article/Active-Shooter-Pay-Attention-to-Emergency-Notification

8. ACCOUNTABILITY



Accountability is the process through which an organization determines the status and location of personnel following an incident, aiding recovery efforts and facilitating family notifications.

Personnel and Procedures

Personnel Responsible for Accountability

Organizations should maintain updated personnel rosters and provide them to those responsible for accountability during an active assailant incident. Organizations should also identify a group responsible for initiating accountability of the organization's personnel. During an emergency, these individuals are responsible for gathering and sharing information on the location and status, if known, of organizational personnel to leadership, law enforcement, and other first responders, as necessary.

Accountability Procedures

Organizations should develop procedures to account for all personnel, visitors, and vendors/contractors during and after an emergency. This includes establishing multiple communication methods to enable personnel to relay their status to those responsible for accountability. Due to today's mobile workforce, this can be challenging. Each person's unique circumstances during an incident can impact their ability to provide a timely response. In the immediate aftermath of an active assailant incident, it may take a considerable amount of time to completely account for all personnel. Accountability procedures should clearly state how personnel will relay their status.

When developing accountability procedures, consider the following:

- Establish clear sign-in protocols for visitors, patrons, vendors, and contractors.
- Designate individual(s) responsible for accountability.
- Identify safe and secure assembly areas (e.g., reunification, information, and family assistance centers).
- Identify individual(s) responsible for sharing personnel status and location with leadership, law enforcement, and/or emergency officials.
- Establish protocols for sharing accountability information with law enforcement.
- Identify method(s) personnel will use to provide status updates.
- Establish a process for notifying next of kin.
- Prepare for communication delays by conducting routine system tests and implementing multiple communication methods.



EXAMPLE — Accountability Procedures Section:

Once an active assailant alert is issued and staff respond, the leadership team and law enforcement must receive rapid and complete accountability information from all personnel to determine their status and location.

When it is safe to do so, initiate accountability through the following actions:

- Management will initiate accountability procedures.
- Personnel will provide status to management in accordance with organizational procedures.
- Management will contact individuals who have not provided their status.

**To learn more about accountability, review the following resources:**

- CISA, Active Shooter Emergency Action Plan Product Suite, cisa.gov/resources-tools/resources/active-shooter-emergency-action-plan-product-suite
- CISA, ISC, Occupant Emergency Programs Guide, cisa.gov/resources-tools/resources/isc-occupant-emergency-programs-guide
- CISA, ISC, Planning and Response to an Active Shooter Guide, cisa.gov/resources-tools/resources/isc-planning-and-response-active-shooter-guide
- OSHA, Evacuation Plans and Procedures e-Tool, Emergency Action Plan – Evacuation Elements, osha.gov/etools/evacuation-plans-procedures/eap/elements



9. RECOVERY



Recovery is the process of transitioning from crisis response to normality... and it's a new "normal."

Once the active assailant threat has been neutralized, the lengthy process of recovery begins. This process is continuous and occurs in both short- and long-term incremental phases. Organizations should develop recovery plans and procedures to help them resume operations and provide personnel and community members with the necessary support following an incident.

Recovery Planning

Managing the immediate aftermath of an active assailant incident relies on rapidly implementing a recovery plan that ensures people are safe, accounted for, and reunited with their families. Recovery also requires a holistic approach to ensure the needs of those impacted are addressed. With no set timetable for any one person's or community's recovery, the process can last for months or even years after the incident. Recovery is resource intensive and having a recovery plan can facilitate an organization's preparedness for the aftermath of an active assailant attack.

An effective recovery plan can also complement business continuity. In many cases, the physical site may be inaccessible for an extended period after an active assailant attack, which can directly impact employees' ability and willingness to work, as well as the organization's ability to operate. It is critical for organizations to commit to developing a recovery plan that addresses the needs of its people and a plan that addresses business continuity.

When developing elements of a recovery plan, consider the following:

- Designate individuals responsible for implementing the recovery plan and outline roles and responsibilities.
- Determine how the organization will communicate with employees and provide services in the aftermath of an active assailant incident.
- Ensure recovery services can be leveraged by traditionally underserved members of a community, as well as those whose primary language may not be English.

Community Resources

Recovering from an active assailant incident is a community effort. It may include hospitals and other medical facilities, grief counselors, employee assistance programs, faith-based organizations, lawyers, and insurance providers, among others. Organizations should coordinate with community leaders to confirm availability of resources, as well as collaborate with businesses or organizations who may be impacted by the incident or are able to provide recovery services or resources to impacted personnel.

When engaging community resources, consider the following:

- Determine what support services will be needed.
- Create a detailed inventory of available resources and relevant contact information.
- Establish service agreements with external organizations to enable timely provision of support.
- Determine estimated costs associated with support services.
- Document the timeline and process for implementing identified services.
- Periodically review and update resource information and service agreements with supporting resource providers.



Short-Term Recovery

Short-term recovery generally occurs in the first few hours and days following an incident. Primary goals for short-term recovery include reestablishing safety and mitigating the physical, psychological, and emotional impacts of the incident.

When developing short-term recovery procedures, consider the following:

- Provide for the health and safety needs of personnel, family, and others.
- Provide access to support services (e.g., mental health, spiritual).
- Establish reunification protocols for families and communities.
- Create a hotline and crisis communications center for information sharing.
- Leverage criminal justice-based victim services, as appropriate.
- Help plan any necessary funerals, vigils, and/or memorial services.
- Identify business continuity plans and alternate locations for operations, if necessary.
- Develop an after-action report that documents lessons learned from the incident response.

Mid- to Long-Term Recovery

Mid- to long-term recovery focuses on restoring services and adjusting to a “new normal.” It generally begins when the organization and community’s immediate short-term needs have been addressed. Mid- to long-term recovery can take anywhere from months to years and depends on the organization and the individuals affected, as well as the specific circumstances of the incident. The goal during mid- to long-term recovery is restoring services and helping those impacted resume their daily lives.

When developing mid- to long-term recovery procedures, consider the following:

- Provide long-term grief counseling services.
- Identify key resources and personnel required to resume operations.
- Manage donations, such as money, goods, and services.
- Maintain awareness of potential scams and fraudulent activity during the recovery process.
- Identify methods to support the legal/judicial process.
- Plan for long-term memorials, vigils, and remembrances.
- Review and update recovery plans following an incident.



Business Continuity

Business continuity is an organization's ability to resume operations following an incident or disruption. An active assailant incident can significantly impact an organization's ability to continue operating, and in some cases, may result in the organization having to cease operations entirely. Organizations should plan for how they will function immediately following an incident, as well as in the months and years to follow. The condition of the facility and the status of personnel may also impact an organization's ability to continue operations.

When developing elements of a business continuity plan, consider the following:

- Determine how long the organization can withstand a disruption to daily business operations.
- Determine how the organization will sustain or re-establish its most essential business functions following an incident.
- Identify a process to provide updates on the status of facility or organizational operations.
- Create plans to protect critical information, records, and IT systems.
- Develop a plan for ensuring the safety of organization personnel.
- Determine if business operations can resume at the impacted site.
- Identify alternate work sites if the impacted site has sustained too much damage, is considered unsafe for use, or is still an active crime scene.
- Establish necessary agreements for alternate work locations in advance of a crisis or incident.
- Assess the organization's ability to address personnel absences, if necessary.
- Analyze legal and financial considerations that could impact business operations.

To learn more about recovery, review the following resources:

- CISA, Active Shooter Preparedness, [cisa.gov/topics/physical-security/active-shooter-preparedness](https://www.cisa.gov/topics/physical-security/active-shooter-preparedness)
- CISA, Active Shooter Recovery Guide, [cisa.gov/resources-tools/resources/active-shooter-recovery-guide](https://www.cisa.gov/resources-tools/resources/active-shooter-recovery-guide)
- CISA, Crisis Event Response and Recovery Access (CERRA) Framework, [cisa.gov/sites/default/files/2023-12/crisis-event-response-and-recovery-access-framework_112023_508.pdf](https://www.cisa.gov/sites/default/files/2023-12/crisis-event-response-and-recovery-access-framework_112023_508.pdf)
- CISA, Critical Manufacturing Sector Active Assailant Post-Incident Best Practices Guide, [cisa.gov/resources-tools/resources/critical-manufacturing-sector-active-assailant-post-incident-best-practices-guide](https://www.cisa.gov/resources-tools/resources/critical-manufacturing-sector-active-assailant-post-incident-best-practices-guide)
- CISA, Insider Threat Mitigation, [cisa.gov/topics/physical-security/insider-threat-mitigation](https://www.cisa.gov/topics/physical-security/insider-threat-mitigation)
- CISA, ISC Planning and Response to an Active Shooter Guide, [cisa.gov/resources-tools/resources/isc-planning-and-response-active-shooter-guide](https://www.cisa.gov/resources-tools/resources/isc-planning-and-response-active-shooter-guide)
- DOJ, Office for Victims of Crime: Helping Victims of Mass Violence & Terrorism Planning, Response, Recovery, and Resources, ovc.ojp.gov/sites/g/files/xyckuh226/files/pubs/mvt-toolkit/about-toolkit.html
- FBI, Developing Emergency Operations Plans: A Guide for Businesses, [fbi.gov/file-repository/active-shooter-guide-for-businesses-march-2018.pdf/view](https://www.fbi.gov/file-repository/active-shooter-guide-for-businesses-march-2018.pdf/view)
- FBI, Victim Assistance Services, [fbi.gov/how-we-can-help-you/victim-services](https://www.fbi.gov/how-we-can-help-you/victim-services)
- FEMA, Emergency Management - Community Recovery Management Toolkit, [fema.gov/emergency-managers/practitioners/recovery-resources/community-toolkit](https://www.fema.gov/emergency-managers/practitioners/recovery-resources/community-toolkit)
- I Love U Guys Foundation, The Standard Reunification Method, [iloveuguy.org/The-Standard-Reunification-Method.html](https://www.iloveuguy.org/The-Standard-Reunification-Method.html)
- Private Sector Preparedness Response and Recovery (PSPR2) Seminar Series Recordings, [vimeo.com/showcase/pspr2](https://www.vimeo.com/showcase/pspr2)
- Substance Abuse and Mental Health Services Administration (SAMSHA), [samhsa.gov](https://www.samhsa.gov)

10. TRAINING AND EXERCISES



During an active assailant incident, personnel will likely rely on their baseline training to help them respond effectively. Training, exercises, and drills are essential components of an organization's EAP, as these help to build muscle memory to enable more effective responses during an active assailant incident. Staff and volunteers should be trained on best practices for surviving an active assailant incident. In an emergency, people who are untrained and under extreme stress may freeze, panic, or make decisions that can lead to injury or loss of life.

To ensure personnel are fully engaged and able to act, organizations should consider developing and implementing a training plan that includes an exercise component. Exercises provide a simulated environment in which an organization can test and validate existing plans and procedures, while simultaneously identifying gaps in plans, training deficiencies, and resource shortfalls before an active assailant incident occurs. Organizations should include emergency responders from local or regional agencies during training and exercises to reinforce collaboration, build emergency responder familiarity with the facility, and improve the organization's response proficiency.

Individuals Responsible for Training

Organizations should establish a training team tasked with ensuring personnel are trained and informed on how to respond to an active assailant incident. The size of the team can vary based on the organization's size, mission, and available resources.

When identifying individual(s) responsible for training personnel, organizations should consider the following:

- The type of training the organization will use (e.g., in-person, virtual, video-based).
- The individual's ability to manage a training program.
- Prior training experience.
- The trainer's knowledge and understanding of the topic, as well as the purpose for the training.

Training

For training to be effective, it must be conducted on a routine basis to ensure staff are prepared to effectively respond during an active assailant incident. Training methods can include online learning, tabletop exercises, and/or full-scale exercises. When identifying training resources, organizations should consider response models such as [Run-Hide-Fight](#), and life-saving first-aid training such as [Stop the Bleed®](#). Organizations should ensure training materials are relevant, current, and applicable. Training across the organization must be consistent and uniform to ensure all personnel are learning the same information and following the same response procedures. This is especially relevant for organizations with multiple sites and facilities, such as multinational corporations, school districts, and franchises.



When developing training procedures, consider the following:

- Identify the training staff will require.
- Determine how and when staff will be trained to ensure:
 - Understanding of threat types and hazards that may occur.
 - Understanding of individual responsibilities and actions for training staff.
 - Consensus around how often employees will be trained (e.g., annually, semi-annually, or more frequently).
- Determine training methods, such as web-based, video training, virtual, or in-person.
- Implement methods for monitoring, recording, and tracking training.
- Determine how and when training will be conducted (e.g., annually and/or at onboarding).
- Assess training curriculum to ensure information remains current and relevant.
- Establish the frequency of drills and exercises.
- Conduct reviews after completing drills and exercises.
- Consider individual responses to an active assailant incident, such as:
 - Where do we run?
 - Where do we hide?
 - How do we fight?

Exercises

Organizations should regularly exercise their EAP as this provides effective and practical mechanisms to identify areas for improvement, as well as best practices. When possible, consider including partner organizations, such as local law enforcement, fire, or co-located organizations/businesses as they may have important information to contribute as you discuss your EAP.

When incorporating exercises into a training program, consider the following:	
<p>Tabletop exercises are discussion-based exercises where team members meet in an informal setting to discuss their roles and responses during an emergency, based on their understanding of the EAP. Tabletop exercises involve less planning and coordination than other exercises, can be conducted on a smaller scale, and can be used to focus on specific elements of the EAP (such as response, recovery, communications, etc.).</p>	<p>Functional exercises allow personnel to validate plans and readiness by performing their duties in a simulated environment. Activities for a functional exercise are scenario-driven, such as the failure of a critical business function or a specific hazard scenario. Functional exercises are designed to test specific team members, procedures, and resources (e.g., communication, warning, notification, and equipment set-up).</p>
<p>Full-scale exercises are scenario-based, involve more complex elements, and can take up to 18 months to plan. Organizations should include law enforcement, fire departments, emergency management personnel, and security professionals when implementing a full-scale exercise.</p>	<p>After Action Report (AAR) is a document intended to capture observations of an exercise and make recommendations for post-exercise improvements. The final AAR and Corrective Action Plan are used to address any areas for improvement identified during the exercise, as well as capture best practices that can be modeled across the organization.</p>

**When developing exercise procedures, consider the following:**

- Set the timeframe for developing scenario-based exercises.
- Identify the type of scenario to be considered.
- Establish safety measures when conducting the scenario-based exercise.
- Implement notification procedures for personnel, patrons, visitors, contractors/vendors, and surrounding businesses.
- Collaborate with local/regional officials including first responders for assistance with planning full-scale exercises.
- Develop an After Action Report based on discussions or actions from exercises.
- Develop a Corrective Action Plan and share with key authorized personnel.

To learn more about training and exercise development, review the following resources:

- CISA, Active Shooter Preparedness - Active Shooter Preparedness Webinar Training, cisa.gov/resources-tools/training/active-shooter-preparedness-webinar
- CISA, Active Shooter Preparedness: Options for Considerations Video, cisa.gov/resources-tools/resources/options-consideration-video
- CISA, Exercises, cisa.gov/about/divisions-offices/cisa-exercises
- DHS, Ready.gov, Business Training – Training and Testing: Exercises, ready.gov/business/training/testing-exercise/exercises
- DHS, School and Workplace Violence, dhs.gov/school-and-workplace-violence
- DHS, STOP THE BLEED®, dhs.gov/stopthebleed
- FEMA, EMI: IS-907: Active Shooter: What You Can Do, training.fema.gov/is/courseoverview.aspx?code=IS-907&lang=en
- FEMA, EMI: NIMS Training Program, fema.gov/emergency-managers/nims/implementation-training#training
- FEMA, National Preparedness – Exercise and Preparedness Tools, fema.gov/emergency-managers/national-preparedness/exercises/tools

RESOURCES



Roles and Responsibilities

- CISA, Security Planning Workbook, [cisa.gov/resources-tools/resources/security-planning-workbook](https://www.cisa.gov/resources-tools/resources/security-planning-workbook)
- FEMA, Emergency Management – Planning Guides, [fema.gov/emergency-managers/national-preparedness/plan](https://www.fema.gov/emergency-managers/national-preparedness/plan)
- FEMA, National Incident Management System (NIMS), NIMS Components – Guidance and Tools, [fema.gov/emergency-managers/nims/components](https://www.fema.gov/emergency-managers/nims/components)



Floor Plans and Maps

- CISA, Infrastructure Visualization Platform, [cisa.gov/resources-tools/services/infrastructure-visualization-platform-ivp](https://www.cisa.gov/resources-tools/services/infrastructure-visualization-platform-ivp)
- FBI, Developing Emergency Operations Plans: A Guide for Businesses, [fbi.gov/file-repository/active-shooter-guide-for-businesses-march-2018.pdf/view](https://www.fbi.gov/file-repository/active-shooter-guide-for-businesses-march-2018.pdf/view)
- OSHA, Emergency Action Plan: Evacuation Elements, [osha.gov/etools/evacuation-plans-procedures/eap/elements](https://www.osha.gov/etools/evacuation-plans-procedures/eap/elements)



Facility Emergency Access Preparedness

- CISA, Crisis Event Response and Recovery Access (CERRA) Framework, [cisa.gov/sites/default/files/2023-12/crisis-event-response-and-recovery-access-framework_112023_508.pdf](https://www.cisa.gov/sites/default/files/2023-12/crisis-event-response-and-recovery-access-framework_112023_508.pdf)
- FEMA, Emergency Management – Planning Guides, [fema.gov/emergency-managers/national-preparedness/plan](https://www.fema.gov/emergency-managers/national-preparedness/plan)
- OSHA, Emergency Preparedness and Response: Getting Started, [osha.gov/emergency-preparedness/getting-started](https://www.osha.gov/emergency-preparedness/getting-started)



Emergency Communications

- CISA, Interagency Security Committee (ISC): Planning and Response to an Active Shooter Guide, [cisa.gov/resources-tools/resources/isc-planning-and-response-active-shooter-guide](https://www.cisa.gov/resources-tools/resources/isc-planning-and-response-active-shooter-guide)
- CISA, Priority Telecommunications Services, [cisa.gov/topics/emergency-communications/priority-services](https://www.cisa.gov/topics/emergency-communications/priority-services)
- CISA, Security Planning Workbook, [cisa.gov/resources-tools/resources/security-planning-workbook](https://www.cisa.gov/resources-tools/resources/security-planning-workbook)
- DHS, Ready.gov, Crisis Communications Plans, [ready.gov/business/emergency-plans/crisis-communications-plans](https://www.ready.gov/business/emergency-plans/crisis-communications-plans)
- FBI, Developing Emergency Operations Plans: A Guide for Businesses, [fbi.gov/file-repository/active-shooter-guide-for-businesses-march-2018.pdf/view](https://www.fbi.gov/file-repository/active-shooter-guide-for-businesses-march-2018.pdf/view)
- FEMA, Emergency Management - Comprehensive Preparedness Guide (CPG 101): Developing and Maintaining Emergency Operations Plans, September 2021, [fema.gov/emergency-managers/national-preparedness/plan#cpg](https://www.fema.gov/emergency-managers/national-preparedness/plan#cpg)
- FEMA, NIMS Implementation and Training: NIMS Basic Guidance for Public Information Officers, [fema.gov/emergency-managers/nims/implementation-training#guides](https://www.fema.gov/emergency-managers/nims/implementation-training#guides)
- FEMA, Preparedness Community - Active Shooter: Pay Attention to Emergency Notifications, community.fema.gov/ProtectiveActions/s/article/Active-Shooter-Pay-Attention-to-Emergency-Notification



Procedures for Evacuation, Lockdown, and Shelter-in-Place

- CISA, ISC, Occupant Emergency Programs Guide, cisa.gov/resources-tools/resources/isc-occupant-emergency-programs-guide
- FBI, Developing Emergency Operations Plans: A Guide for Businesses, fbi.gov/file-repository/active-shooter-guide-for-businesses-march-2018.pdf/view
- FEMA, Evacuation and Shelter-in-Place, “Planning Considerations: Evacuation and Shelter-in-Place,” fema.gov/emergency-managers/national-preparedness/plan/evacuation-shelter-in-place
- FEMA, IS-360: “Preparing for Mass Casualty Incidents: A Guide for Schools, Higher Education, and Houses of Worship,” emilms.fema.gov/is_0360/media/276.pdf
- OSHA, Emergency Preparedness and Response: Getting Started, osha.gov/emergency-preparedness/getting-started
- OSHA, Evacuation Plans and Procedures eTool, osha.gov/etools/evacuation-plans-procedures/eap/elements



Response Procedures During an Active Assailant Incident

- CISA, Active Shooter Pocket Card, cisa.gov/resources-tools/resources/active-shooter-pocket-card
- CISA, ISC Planning and Response to an Active Shooter Guide, cisa.gov/resources-tools/resources/isc-planning-and-response-active-shooter-guide
- CISA, Options for Consideration Video, cisa.gov/resources-tools/resources/options-consideration-video
- CISA, Tabletop Exercise Packages (CTEPs), cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages
- CISA, Vehicle Ramming Action Guide, cisa.gov/resources-tools/resources/vehicle-ramming-action-guide
- CISA, Venue Guide for Security Considerations, cisa.gov/resources-tools/resources/venue-guide-security-considerations
- FEMA, Attacks in Crowded and Public Spaces, ready.gov/public-spaces
- FEMA, Evacuation and Shelter-in-Place, “Planning Considerations: Evacuation and Shelter-in-Place,” fema.gov/emergency-managers/national-preparedness/plan/evacuation-shelter-in-place
- FEMA, IS-360: “Preparing for Mass Casualty Incidents: A Guide for Schools, Higher Education, and Houses of Worship,” emilms.fema.gov/is_0360/media/276.pdf
- FEMA, Preparedness Community - Active Shooter: Pay Attention to Emergency Notifications, community.fema.gov/ProtectiveActions/s/article/Active-Shooter-Pay-Attention-to-Emergency-Notification



Accountability

- CISA, Active Shooter Emergency Action Plan Product Suite, cisa.gov/resources-tools/resources/active-shooter-emergency-action-plan-product-suite
- CISA, ISC, Occupant Emergency Programs Guide, cisa.gov/resources-tools/resources/isc-occupant-emergency-programs-guide
- CISA, ISC, Planning and Response to an Active Shooter Guide, cisa.gov/resources-tools/resources/isc-planning-and-response-active-shooter-guide
- OSHA, Evacuation Plans and Procedures e-Tool, Emergency Action Plan – Evacuation Elements, osha.gov/etools/evacuation-plans-procedures/eap/elements



Recovery

- CISA, Active Shooter Preparedness, [cisa.gov/topics/physical-security/active-shooter-preparedness](https://www.cisa.gov/topics/physical-security/active-shooter-preparedness)
- CISA, Active Shooter Recovery Guide, [cisa.gov/resources-tools/resources/active-shooter-recovery-guide](https://www.cisa.gov/resources-tools/resources/active-shooter-recovery-guide)
- CISA, Crisis Event Response and Recovery Access (CERRA) Framework, [cisa.gov/sites/default/files/2023-12/crisis-event-response-and-recovery-access-framework_112023_508.pdf](https://www.cisa.gov/sites/default/files/2023-12/crisis-event-response-and-recovery-access-framework_112023_508.pdf)
- CISA, Critical Manufacturing Sector Active Assailant Post-Incident Best Practices Guide, [cisa.gov/resources-tools/resources/critical-manufacturing-sector-active-assailant-post-incident-best-practices-guide](https://www.cisa.gov/resources-tools/resources/critical-manufacturing-sector-active-assailant-post-incident-best-practices-guide)
- CISA, Insider Threat Mitigation, [cisa.gov/topics/physical-security/insider-threat-mitigation](https://www.cisa.gov/topics/physical-security/insider-threat-mitigation)
- CISA, ISC Planning and Response to an Active Shooter Guide, [cisa.gov/resources-tools/resources/isc-planning-and-response-active-shooter-guide](https://www.cisa.gov/resources-tools/resources/isc-planning-and-response-active-shooter-guide)
- DOJ, Office for Victims of Crime: Helping Victims of Mass Violence & Terrorism Planning, Response, Recovery, and Resources, [ovc.ojp.gov/sites/g/files/xyckuh226/files/pubs/mvt-toolkit/about-toolkit.html](https://www.ovc.ojp.gov/sites/g/files/xyckuh226/files/pubs/mvt-toolkit/about-toolkit.html)
- FBI, Developing Emergency Operations Plans: A Guide for Businesses, [fbi.gov/file-repository/active-shooter-guide-for-businesses-march-2018.pdf/view](https://www.fbi.gov/file-repository/active-shooter-guide-for-businesses-march-2018.pdf/view)
- FBI, Victim Assistance Services, [fbi.gov/how-we-can-help-you/victim-services](https://www.fbi.gov/how-we-can-help-you/victim-services)
- FEMA, Emergency Management - Community Recovery Management Toolkit, [fema.gov/emergency-managers/practitioners/recovery-resources/community-toolkit](https://www.fema.gov/emergency-managers/practitioners/recovery-resources/community-toolkit)
- I Love U Guys Foundation, The Standard Reunification Method, [iloveguys.org/The-Standard-Reunification-Method.html](https://www.iloveguys.org/The-Standard-Reunification-Method.html)
- Private Sector Preparedness Response and Recovery (PSPR2) Seminar Series Recordings, [vimeo.com/showcase/pspr2](https://www.vimeo.com/showcase/pspr2)
- Substance Abuse and Mental Health Services Administration (SAMSHA), [samhsa.gov](https://www.samhsa.gov)



Training and Exercises

- CISA, Active Shooter Preparedness - Active Shooter Preparedness Webinar Training, [cisa.gov/resources-tools/training/active-shooter-preparedness-webinar](https://www.cisa.gov/resources-tools/training/active-shooter-preparedness-webinar)
- CISA, Active Shooter Preparedness: Options for Considerations Video, [cisa.gov/resources-tools/resources/options-consideration-video](https://www.cisa.gov/resources-tools/resources/options-consideration-video)
- CISA, Exercises, [cisa.gov/about/divisions-offices/cisa-exercises](https://www.cisa.gov/about/divisions-offices/cisa-exercises)
- DHS, Ready.gov, Business Training – Training and Testing: Exercises, [ready.gov/business/training/testing-exercise/exercises](https://www.ready.gov/business/training/testing-exercise/exercises)
- DHS, School and Workplace Violence, [dhs.gov/school-and-workplace-violence](https://www.dhs.gov/school-and-workplace-violence)
- DHS, STOP THE BLEED®, [dhs.gov/stopthebleed](https://www.dhs.gov/stopthebleed)
- FEMA, EMI: IS-907: Active Shooter: What You Can Do, [fema.gov/is/courseoverview.aspx?code=is-907&lang=en](https://www.fema.gov/is/courseoverview.aspx?code=is-907&lang=en)
- FEMA, EMI: NIMS Training Program, [fema.gov/emergency-managers/nims/implementation-training#training](https://www.fema.gov/emergency-managers/nims/implementation-training#training)
- FEMA, National Preparedness – Exercise and Preparedness Tools, [fema.gov/emergency-managers/national-preparedness/exercises/tools](https://www.fema.gov/emergency-managers/national-preparedness/exercises/tools)