



Delaware Information & Analysis Center

Violent Intruder Toolkit

Quick Reference Guide

Version 1.0 Created: December, 2019

Please Click on
Topic to be
Directed

Policy Development

Training

Exercise Options

Self Assessment

Since the tragic events at Columbine High School on April 20, 1999, "Active Shooter" has evolved into a household term. This single event radically changed school security and the law enforcement profession while also introducing American citizens to an entirely new epidemic of violence. Far too many times active shooter events have occurred on school campuses, in shopping malls, at movie theaters, Houses of Worship and many other peaceful locations. Regrettably hundreds of Americans have fallen to this mass violence epidemic.

This increase in mass violence, however, is not limited to "Active Shooter." Violent Intruder tactics also encompass the use of edge weapons, improvised explosive devices, and the use of vehicles as weapons.

In an effort to develop a comprehensive response to violent intruders, it is important for organizations to address each of the four (4) key areas in this toolkit. The first area, **Policy Development**, provides instruction on the development of a violent intruder policy or emergency action plan, and includes a United States Department of Homeland Security (DHS) template for organizations to follow. The second area, **Training**, discusses suspicious activity reporting and lists several violent intruder training programs available for organizations in Delaware and additional online resources that are available. The third area, **Exercise Options**, provides an overview of the various types of exercise options available to assist in evaluating the policies and responses plans that organizations have in place. The fourth and final area of the toolkit, **Self Assessment**, is a tool for organizations to use to evaluate their security efforts as well as share them with law enforcement representatives for insight and further discussion.

It is our hope that the information and resources included in this toolkit will help your organization further enhance your security posture and help to educate all of the citizens who work/attend/congregate at your facilities. A variety of links are included on each page. Click on the link to be directed to that resource or copy and paste the web address under the image into your browser.

Questions and requests for additional information can be directed to
FORCE12@delaware.gov

DISCLOSURE

This document is "Unclassified//For Official Use Only." All writings, analytical products, guidance, attachments, and templates are the property of the State of Delaware and the Department of Homeland Security. The information contained herein is presented for information sharing purposes only and serves as suggestions and guidance for the implementation of a violent intruder preparation program. This document is not intended to guarantee prevention against manmade / natural threats or acts of destruction or to take the place of any adopted policies and regulations within an existing organization.



Violent Intruder Toolkit

Policy Development



In an effort to help prepare for and respond to a violent intruder incident, organizations are encouraged to develop emergency action plans/policies to help guide the organization in preparedness and response protocols. The United States Department of Homeland Security has developed several guides and templates that organizations can use as they begin creating their own plans/policies.

 Homeland Security

Emergency Action Plan Guide
Active Shooter Preparedness

Purpose

The Active Shooter Emergency Action Plan Video is a virtual learning tool that describes the fundamental concepts of developing an Emergency Action Plan (EAP) for an active shooter scenario. This instructive video guides organizations through important considerations of EAP development utilizing the first-hand perspectives of active shooter survivors, first responders, and other subject matter experts who share their unique insights.

Organizations are encouraged to use this guide as a medium to document the *initial steps* toward creating an Active Shooter preparedness plan. This guide is *not* meant to replace your organization's Emergency Action Plan. Rather, it is a tool that begins the EAP development process.

Pre-Planning Recommendations and Suggested Training

- ✓ Does your organization have an emergency action plan? If so, review your organization's policy or process for creating the plan. Determine if an active shooter preparedness plan can fit into your organization's overarching plan which may already include a plan for fire evacuation, severe weather, and bomb threats.
- ✓ Obtain a copy of the Federal Emergency Management Agency's (FEMA) Comprehensive Preparedness Guide (CPG) 101 ["Developing and Maintaining Emergency Operations Plan"](#) and review the six step planning process.
- ✓ Explore the [Department of Homeland Security's Active Shooter Preparedness Website](#) to better understand the active shooter threat.
- ✓ View the [Options for Consideration Video](#) to recognize possible actions to take if confronted with an active shooter scenario.
- ✓ Download and review the [Active Shooter Preparedness Workshop Series](#) presentations. This six module series contains additional information, instructor notes, and videos that supports the Active Shooter Emergency Action Plan process. The *Planning Steps (1-6)* below will correlate to the Training Modules (1-6) in the presentation slides. Example: *Module 2* will assist with completing *Planning Step 2a* and *2b*.

How to Use This Guide

Step 1 – Review the pre-planning recommendations and suggested training.

Step 2 – Allot *at least 2 hours* to complete the Active Shooter Emergency Action Plan video.

Step 3 – Watch the EAP video.

Step 4 – Complete *Planning Steps 1-6*. Use the fillable space to document the initial steps required to begin developing the organization's Emergency Action Plan. Note: *The Planning Steps contain information derived from the EAP video and other online resources to help inform the planning process.*

Step 5 – Begin drafting the organization's Active Shooter Emergency Action Plan. Refer to the EAP Guide and resources listed in *Pre-Planning Recommendations and Suggested Training* as required.

Need Help? Contact the DHS Active Shooter Preparedness team at ASworkshop@hq.dhs.gov

<https://www.dhs.gov/sites/default/files/publications/active-shooter-emergency-action-plan-112017-508v2.pdf>

Emergency Action Plan Guide

This guide provides the reader with a wealth of resources to assist in the planning, creation, or review of violent intruder emergency action plans/policies. Multiple areas of consideration are addressed for discussion and inclusion in your organization's plans/policies.

To learn more about developing or reviewing a violent intruder policy, please email FORCE12@Delaware.gov

Policy Development

Training

Exercise Options

Self Assessment

Please Click on Topic to be Directed



Violent Intruder Toolkit

Training

“The Homeland will be secure when the Hometown is secure”

Violent Intruder training consists of two general areas that include the recognition of suspicious activity and how to respond during a violent intruder incident. When combined, this training provides citizens with the information to help prevent violent intruder incidents and also increase survivability rates should an incident take place.

Suspicious Activity Reporting

Protect your every day.

RECOGNIZE THE SIGNS OF TERRORISM-RELATED SUSPICIOUS ACTIVITY

The infographic is divided into four sections:

- Expressed or Implied Threat:** Threatening to commit a crime that could harm or kill people within a facility, infrastructure, or secured site.
- Surveillance:** A prolonged interest in taking pictures/videos of personnel, facilities, security features, or infrastructure in an unusual or covert manner.
- Theft/Loss/Diversion:** Stealing or diverting items—such as equipment, uniforms, or bases—that belong to a facility or secured site.
- Testing or Probing of Security:** Investigating or testing a facility's security or IT systems to assess the strength or weakness of the target.
- Aviation Activity:** Operating or interfering with the operation of an aircraft that poses a threat of harm to people and property.

- Breach/Attempted Intrusion:** Unauthorized people trying to enter a restricted area or impersonating authorized personnel.
- Acquisition of Expertise:** Gaining skills or knowledge on a specific topic, such as firearms, military tactics, or flying an aircraft.
- Eliciting Information:** Questioning personnel beyond mere curiosity about an event, facility, or operations.
- Misrepresentation:** Presenting false information or misusing documents to conceal possible illegal activity.
- Cyberattack:** Disrupting or compromising an organization's information technology systems.

- Recruiting/Financing:** Funding suspicious or criminal activity or recruiting people to participate in criminal or terrorist activity.
- Sabotage/Tampering/Vandalism:** Damaging or destroying part of a facility, infrastructure, or secured site.
- Materials Acquisition/Storage:** Acquisition and/or storage of unusual materials, such as cell phones, radio controllers, or toxic materials.
- Weapons Collection/Storage:** Collection or discovery of unusual amounts of weapons, including explosive chemicals or other destructive materials.
- Sector-Specific Incident:** Actions which raise concern to specific sectors, (e.g., power plants, chemical plants) regard to their personnel, facilities, systems, or functions.

If you see something, say something®
REPORT SUSPICIOUS ACTIVITY TO LOCAL AUTHORITIES OR CALL 911 IN CASE OF EMERGENCY

dhs.gov/see-something-say-something

“If You See Something, Say Something®” used with permission of the FBI/Interstate Emergency Authority.

The United States Department of Homeland Security has a variety of resources to familiarize citizens with the signs of a terrorism-related suspicious activities. These resources are available by visiting: <https://www.dhs.gov/see-something-say-something/what-suspicious-activity>. When reporting suspicious activity, it is important to pay attention to “5W’s”:

- Who did you see?
- What did you see?
- When you saw it?
- Where it occurred?
- Why is it suspicious?

In an emergency, call 911. If the information is not an emergency, suspicious activity can be reported in any of the following ways:

Call: 1-800-FORCE-1-2

Email: FORCE12@Delaware.gov

Website: DE Terrorism Tip Link

<https://www.dhs.gov/see-something-say-something/recognize-the-signs>

Policy Development

Training

Exercise Options

Self Assessment

Please Click on Topic to be Directed



Violent Intruder Toolkit

Training

“The Homeland will be secure when the Hometown is secure”

Training Programs Available in Delaware

There are three (3) main training programs available in Delaware citizens on the topic of violent intruder response. Below is a summary of each training program and links to find additional information. To learn more about which option is right for you, please email FORCE12@Delaware.gov

CRASE: Civilian Response to Active Shooter Events (CRASE). Law enforcement officers and agencies are frequently requested by schools, businesses, and community members for direction and presentations on what they should do if confronted with an active shooter event. The Civilian Response to Active Shooter Events (CRASE) course, designed and built on the [Avoid, Deny, Defend](#) (ADD) strategy developed by the Advanced Law Enforcement Rapid Response Training (ALERRT) in 2004, provides strategies, guidance, and a proven plan for surviving an active shooter event. To learn more visit: <http://www.avoiddenydefend.org/>

VIPR: The Violent Intruder Preparedness & Response (VIPR). This training program is Delaware-based program designed for unarmed citizens and built on the [“Run, Hide, Fight”](#) strategy that has been recognized as an industry standard. The VIPR training objectives are simple yet effective. The key concepts of the VIPR program are to 1) Increase situational awareness of active shooter events; 2) Encourage organizations to have emergency action plans that are shared with employees and rehearsed; 3) Provide practical examples of barricading confined spaces and considerations for utilizing self-defense options; 4) Demonstrate basic emergency casualty care tactics for the injured. To learn more visit: <https://dediac.org/files/DDF/VIPR%20Program.pdf>

ALICE: Alert, Lockdown, Inform, Counter, Evacuate (ALICE). The threat of an active shooter attack is rare but very real. The program aims to eradicate the “It can’t happen to me” mentality and change the way people in schools, universities, businesses, hospitals and places of worship respond to armed intruders. The ALICE Training Institute believes that individuals should be authorized and empowered to make their own life-saving decisions. Once empowered to make their own life-saving decisions, individuals must be trained in proactive response options, rather than a passive, mandated, one size fits all response. The ALICE Training Institute wants all Americans to have the knowledge and skills to survive when shots are fired. The program achieves this by training as many people as possible and implementing training in drill form. To learn more visit: <https://www.alicetraining.com/>

Online Resources

In addition to the above resources, there are wealth of resources available to citizens by visiting <https://www.dhs.gov/cisa/active-shooter-preparedness>. This website has numerous links and videos that are designed to educate and inform citizens on how to prepare and respond to a violent intruder incident.

The screenshot shows the homepage of the Homeland Security CISA Active Shooter Preparedness website. The header includes the DHS logo and the text 'CISA' and 'CISA | Cybersecurity and Infrastructure Security Agency'. The main navigation menu includes 'Home CISA', 'Compliance', 'Information Security', 'Emergency Management', 'National Risk Management', and 'About DHS'. Below the menu, a section titled 'Action Shooter Preparedness' is visible, featuring a sub-menu with links to 'First Responders', 'Human Resources or Security Professionals', 'Private Sector', 'Active Shooter Workshop Participants', 'Transgender Active Shooter Resources', 'Interfaith Emergency Resources', and 'Active Shooter Response Resources'. A sidebar on the right provides information about active shooter incidents and links to 'First Responders', 'Human Resources or Security Professionals', 'Private Sector', and 'Active Shooter Workshop Participants'.

Policy Development

Training

Exercise Options

Self Assessment

Please Click on Topic to be Directed

Violent Intruder Toolkit



Exercise Options

Once a violent intruder response plan/policy has been created and adopted by an organization and the members of that organization have been trained, it is important for members of that organization to exercise on the prevention, protection and response of the plan. The United States Department of Homeland Security (DHS) has established the Homeland Security Exercise and Evaluation Program (HSEEP) to help provide a standardized policy, methodology, and terminology for the exercise design, development, conduct, evaluation, and improvement planning.

According to the HSEEP, there are seven (7) different types of exercises which are broken down into either discussion-based exercise or operations-based exercise. These exercises serve to familiarize participants with plans, policies, and procedures.

Types of "Discussion-Based" Exercises:

- **Seminar:** A seminar is an informal discussion, designed to orient participants to new or updated plans, policies, or procedures.
- **Workshop:** A workshop resembles a seminar, but is employed to build specific products, such as a draft plan or policy.
- **Tabletop Exercise (TTX):** A tabletop exercise involved key personnel discussing simulate scenarios in an informal setting. TTXs can be used to assess plans, policies, and procedures.
- **Games:** a game is a simulation of operations that often involves two or more teams, usually in a competitive environment, using rules, data, and procedure designed to depict an actual or assumed real-life situation.

Types of "Operations-Based" Exercises:

- **Drill:** A drill is a coordinated, supervised activity usually employed to test a single, specific operation or function within a single entity.
- **Functional Exercise (FE):** A functional exercise examines and/or validates the coordination, command, and control between various multi-agency coordination centers. A functional exercise does not involve first responders participating.
- **Full-Scale Exercise (FSE):** A full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional and first responder response.

To learn more about which exercise option is right for you, please
email FORCE12@Delaware.gov



Homeland Security Exercise and Evaluation Program (HSEEP)

April 2013



https://www.fema.gov/media-library-data/20130726-1914-25045-8890/hseep_apr13.pdf

Policy Development

Training

Exercise Options

Self Assessment

Please Click on Topic to be Directed



Violent Intruder Toolkit

Self Assessment



The Security Assessment Report has been designed by the Delaware Information and Analysis Center (DIAC) to provide your organization with a self-assessment guide to follow to identify vulnerabilities at your facility. Based on your input, an analysis will be performed and recommendations will be made for you to use to develop a safer environment for your employees and visitors and share with your local law enforcement agency.

Please be sure to complete all sections in the report to ensure a detailed analysis. If you have any questions, please contact DIAC by emailing FORCE12@Delaware.gov. Upon completion, please forward the document to FORCE12@Delaware.gov so that it can be reviewed by critical infrastructure assessment specialist.

To download the Self-Assessment Guide click the link below and select "Save As" and select a location to store the document on your computer.

<https://dediac.org/files/DDF/SELF-ASSESSMENT%20FORM.docx>

Delaware Information and Analysis Center



Critical Infrastructure Unit Security Assessment Report

**FACILITY NAME
ADDRESS
DATE**

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Instructions to Complete the Security Self-Assessment

- 1.) Download the document from the above link and save to your computer.
- 2.) Print out the document and begin compiling the materials required for completion. The assessment is broken down into the following areas:
 - Site Identification (general site information)
 - Identification of Site Operations
 - Threat Identification
 - Security Checklists
 - Attachments to Include Floor Plans and Photos
- 3.) Upon completing the document and including all of the required information, send completed copy via email to FORCE12@Delaware.gov.
- 4.) A critical infrastructure assessment specialist will review your self-assessment and contact you to discuss the findings and consult on next steps.

To learn more about the Security Self-Assessment, please email
FORCE12@Delaware.gov

Policy Development

Training

Exercise Options

Self Assessment

Please Click on Topic to be Directed