# Table of Contents

## 1 Resource Matrix
- For Everyone .................................................. 5
- For Businesses .................................................. 6
- For Government ............................................... 7
- For First Responders .......................................... 7

## 2 Resource Descriptions & Links
- Understand the Basics ......................................... 9
- Identify Suspicious Behavior ................................ 10
- Protect, Screen, and Allow Access to Facilities .......... 11
- Protect Against Unmanned Aircraft Systems ............. 13
- Prepare and Respond to Active Assailants ................. 13
- Prevent and Respond to Bombings ......................... 15
- Connect with the Office of Infrastructure Protection .... 17

## 3 Contacts .......................................................... 19
1 Resource Matrix

Segments of our society are inherently open to the general public, and by nature of their purpose do not incorporate strict security measures. Given the increased emphasis by terrorists and other extremist actors to leverage less sophisticated methods to inflict harm in public areas, it is vital that the public and private sectors collaborate to enhance security of locations such as transportation centers, parks, restaurants, shopping centers, special event venues, and similar facilities. Securing these locations and venues is essential to preserving our way of life and sustaining the engine of our economy. The Office of Infrastructure Protection (IP), part of the U.S. Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD), is committed to improving the security and resilience of soft targets by providing relevant tools, training, and programs to both the public and private sectors, and the general public. This guide is a catalog of IP soft target resources, many of which were created in collaboration with our partners to ensure they are useful and reflective of the dynamic environment we live in.

Legend: Type of Resource

<table>
<thead>
<tr>
<th>Type of Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fact Sheet</td>
</tr>
<tr>
<td>Guide</td>
</tr>
<tr>
<td>Informational Materials</td>
</tr>
<tr>
<td>In-Person Training</td>
</tr>
<tr>
<td>Online Training</td>
</tr>
<tr>
<td>Tool</td>
</tr>
<tr>
<td>Video</td>
</tr>
<tr>
<td>Website</td>
</tr>
</tbody>
</table>

For Everyone

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>RESOURCE</th>
<th>TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand the Basics</td>
<td>Tools and Resources to Help Businesses Plan, Prepare, and Protect from an Attack</td>
<td></td>
</tr>
<tr>
<td></td>
<td>“If You See Something, Say Something” Campaign® Informational Video and Radio PSA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>“If You See Something, Say Something” Campaign® Informational Print Materials PSA</td>
<td></td>
</tr>
<tr>
<td>Identify Suspicious Behavior</td>
<td>Insider Threat Video</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pathway to Violence Action Guide</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pathway to Violence Video</td>
<td></td>
</tr>
<tr>
<td></td>
<td>What’s in Store: Ordinary People, Extraordinary Events Video</td>
<td></td>
</tr>
<tr>
<td>Protect Against Unmanned Aircraft Systems</td>
<td>Unmanned Aircraft Systems (UAS) Critical Infrastructure Drone Pocket Card</td>
<td></td>
</tr>
<tr>
<td></td>
<td>UAS Frequently Asked Questions</td>
<td></td>
</tr>
<tr>
<td>Prepare and Respond to Active Assailants</td>
<td>Active Shooter Booklet</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Active Shooter Preparedness Program Website</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Active Shooter Event Quick Reference Guide</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Active Shooter Poster</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Active Shooter Pocket Card</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Options for Consideration Active Shooter Preparedness Video</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Vehicle Ramming Attack Mitigation Video</td>
<td></td>
</tr>
<tr>
<td>CATEGORY</td>
<td>RESOURCE</td>
<td></td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Understand the Basics</td>
<td>Business Continuity Planning Suite</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Independent Study Training Courses</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sector-Specific Tabletop Exercise Program (SSTEP)</td>
<td></td>
</tr>
<tr>
<td>Identify Suspicious Behavior</td>
<td>Bomb-Making Materials Awareness Program (BMAP)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Nationwide Suspicious Activity Reporting (SAR) Initiative – Private Sector Security</td>
<td></td>
</tr>
<tr>
<td></td>
<td>No Reservations: Suspicious Behavior in Hotels Video</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Suspicious Behavior Advisory Posters</td>
<td></td>
</tr>
<tr>
<td>Protect, Screen, and Allow Access to Facilities</td>
<td>At-A-Glance Guide for Protecting Faith-Based Venues</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Check It! – Bag Check Video</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Evacuation Planning Guide for Stadiums</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Patron Screening Best Practices Guide</td>
<td></td>
</tr>
<tr>
<td>Protect Against Unmanned Aircraft Systems</td>
<td>Protective Measures Guides</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sports Venue Bag Search Procedures Guide</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sports Venue Credentialing Guide</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Vehicle-Borne Improvised Explosive Device (IED) Identification Guide</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Vehicle Inspection Guide</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Vehicle Inspection Video</td>
<td></td>
</tr>
<tr>
<td>Prepare and Respond to Active Assailants</td>
<td>Unmanned Aircraft Systems: Addressing Critical Infrastructure Security Challenges</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unmanned Aircraft Systems – Critical Infrastructure Video</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Active Shooter Preparedness In-Person Workshops</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Active Shooter Emergency Action Planning Guide</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Active Shooter Emergency Action Planning Template</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Active Shooter Emergency Action Planning Video</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Active Shooter Recovery Guide</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Recovering From An Active Shooter Incident Action Guide</td>
<td></td>
</tr>
</tbody>
</table>
### Legend: Type of Resource

- Fact Sheet
- Guide
- Informational Materials
- In-Person Training
- Online Training
- Tool
- Video
- Website

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>RESOURCE</th>
<th>TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevent and Respond to Bombings</td>
<td>Counter-IED and Risk Mitigation Training</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sports and Entertainment Venues Bombing Prevention Solutions Portfolio</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Technical Resource for Incident Prevention (TRIPwire) Website</td>
<td></td>
</tr>
<tr>
<td></td>
<td>What to Do – Bomb Threat Website</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Bomb Threat Procedures Checklist</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Bombing Prevention Lanyard Cards</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DHS-Department of Justice (DOJ) Bomb Threat Guidance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>What You Can Do When There is a Bomb Threat Video</td>
<td></td>
</tr>
<tr>
<td>Connect with the Office of Infrastructure Protection</td>
<td>Homeland Security Information Network – Critical Infrastructure (HSIN-CI)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IP Regional Offices</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Assist Visits and the Infrastructure Survey Tool</td>
<td></td>
</tr>
</tbody>
</table>

#### For Government

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>RESOURCE</th>
<th>TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect, Screen, and Allow Access to Facilities</td>
<td>Interagency Security Committee Best Practices for Mail Screening and Handling Processes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Occupant Emergency Programs: An Interagency Security Committee Guide</td>
<td></td>
</tr>
<tr>
<td>Prepare and Respond to Active Assailants</td>
<td>Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practices Guide</td>
<td></td>
</tr>
<tr>
<td>Prevent and Respond to Bombings</td>
<td>Multi-Jurisdictional Improvised Explosive Device (IED) Security Planning</td>
<td></td>
</tr>
<tr>
<td>Connect with the Office of Infrastructure Protection</td>
<td>Interagency Security Committee</td>
<td></td>
</tr>
</tbody>
</table>

#### For First Responders

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>RESOURCE</th>
<th>TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect, Screen, and Allow Access to Facilities</td>
<td>Crisis Event Response and Recovery Access (CERRA) Framework</td>
<td></td>
</tr>
<tr>
<td>Protect Against Unmanned Aircraft Systems</td>
<td>Unmanned Aircraft Systems: Considerations for Law Enforcement</td>
<td></td>
</tr>
</tbody>
</table>
2 Resource Descriptions & Links

This section includes brief descriptions of each of the available resources and includes links to the resources or where you can find more information.

Understand the Basics

The following resources provide an introduction to facility security and can serve as a good first step for businesses. Resources include fact sheets, guidance, and online training and education courses that cover topics such as Implementing Critical Infrastructure Security and Resilience Programs and Workplace Security Awareness.

Tools and Resources to Help Businesses Plan, Prepare, and Protect from an Attack
Provides business owners and their employees with an overview of the Hometown Security Initiative, specifically how to apply the four steps: Connect, Plan, Train, and Report to their workplace and communities. The Hometown Security Report Series (HSRS) provides reports on community infrastructure and institutions, including commercial office buildings, commuter rail systems, hotels, hospitals, and institutes of higher education. The reports are one of the free tools and resources provided under the initiative.

Link: https://www.dhs.gov/hometown-security

Audience 📋 📚 Type 📚

Independent Study Training Courses
Provide individuals, businesses, first responders, and law enforcement with the information needed to improve security at their facilities. The self-paced, online courses hosted by the Federal Emergency Management Agency's (FEMA) Emergency Management Institute cover topics such as levels of protection and design-basis threat, active shooter, insider threat, workplace security, hidden hazards in retail spaces, and suspicious activity surveillance. All courses require a FEMA student identification number. For more information on how to register, please visit: https://cdp.dhs.gov/femasid/register.

Link: https://training.fema.gov/is/

Audience 📋 📚 Type 📚

Business Continuity Planning Suite
Helps businesses create, improve, or update their business continuity plan to reduce the potential impact of a disruption to business. The suite includes business continuity planning training, business continuity and disaster recovery plan generators, and a business continuity plan validation.

Link: https://www.ready.gov/business-continuity-planning-suite

Audience 📌 📋 📚 Type 📚

Sector-Specific Tabletop Exercise Program (SSTEP)
Assists the critical infrastructure community in conducting their own tabletop exercises by allowing users to leverage pre-built exercise templates and tailor them to their specific needs in order to assess, develop, and update emergency action plans, programs, policies and procedures. These resources provide exercise planners with tools, scenarios, question sets, and guidance to support the development of a discussion-based exercise. There are over 30 SSTEP exercise templates, including ones for outdoor events and insider threats.

Link: https://hsin.dhs.gov/ci/sites/exerciseinfo/Pages/SSTEPS.aspx

Audience 📌 📋 📚 Type 📚
## Identify Suspicious Behavior

These resources help all citizens, business owners and employees, and private sector security personnel understand what suspicious behaviors may pose a threat and what steps to take to report the behavior to authorities.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Nationwide Suspicious Activity Reporting (SAR) Initiative – Private Sector Security Training</strong></td>
<td>Assists private sector security personnel in recognizing what kind of suspicious behaviors are associated with pre-incident terrorism activities, understanding how and where to report suspicious activities, and protecting privacy, civil rights, and civil liberties when documenting information.</td>
<td><a href="https://nisi.ncirc.gov/hsptregistration/private-sector/">https://nisi.ncirc.gov/hsptregistration/private-sector/</a></td>
</tr>
<tr>
<td><strong>No Reservations: Suspicious Behavior in Hotels Video</strong></td>
<td>Helps hotel employees identify and report suspicious activities and threats in a timely manner by highlighting the indicators of suspicious activity. The video is also available in Spanish.</td>
<td><a href="https://www.dhs.gov/video/no-reservations-suspicious-behavior-hotels">https://www.dhs.gov/video/no-reservations-suspicious-behavior-hotels</a></td>
</tr>
<tr>
<td><strong>“If You See Something, Say Something” Campaign®</strong></td>
<td>Provides outreach materials such as posters, brochures, and Web graphics that can be provided to partners at no cost to help raise public awareness of the indicators of terrorism and terrorism-related crime. Also available are video and radio public service announcements to raise public awareness of the indicators of terrorism and terrorism-related crime. The public service announcements are available in English and Spanish, but the U.S. Department of Homeland Security (DHS) is able to work with partners to address specific language needs. The topics include Protect Your Everyday for all citizens, Hospitality for travelers and owners and operators of hotels, and Officials focused on the major sport leagues.</td>
<td><a href="https://www.dhs.gov/sites/default/files/publications/dhs-pathway-to-violence-09-15-16-508.pdf">https://www.dhs.gov/sites/default/files/publications/dhs-pathway-to-violence-09-15-16-508.pdf</a></td>
</tr>
<tr>
<td><strong>Pathway to Violence Action Guide</strong></td>
<td>Explains warning signs that may lead to violence and what individuals can do to mitigate a potential incident.</td>
<td><a href="https://www.dhs.gov/pathway-violence-video">https://www.dhs.gov/pathway-violence-video</a></td>
</tr>
<tr>
<td><strong>Pathway to Violence Video</strong></td>
<td>Identifies behavior indicators that assailants often demonstrate before a violent act based on expert research. The video describes the six progressive steps that may be observable by colleagues, engagement strategies, and recommended responses.</td>
<td><a href="https://www.dhs.gov/pathway-violence-video">https://www.dhs.gov/pathway-violence-video</a></td>
</tr>
<tr>
<td><strong>Suspicious Behavior Advisory Posters</strong></td>
<td>Serve as a quick-reference resource to help businesses, first responders, and local governments identify suspicious activities and behaviors and prevent the illicit sale of explosive precursor chemicals and components. The posters are available under the Suspicious Activities and Bomb Threats – What to Do section of the TRIPwire Website.</td>
<td><a href="https://tripwire.dhs.gov/IED/resources/jsp/loginPopup2.jsp">https://tripwire.dhs.gov/IED/resources/jsp/loginPopup2.jsp</a></td>
</tr>
</tbody>
</table>
Insider Threat Video
Discusses how insider threats manifest in a variety of ways including terrorism, workplace violence, and breaches of cybersecurity. The video can be found under the Insider Threat tab.
Link: https://www.dhs.gov/private-citizen

Bomb-Making Materials Awareness Program (BMAP)
Serves as a source of continued information on Improvised Explosive Device (IED) materials, tactics, and Counter-IED Training. A Community Engagement Website serves as the dashboard for BMAP programs across the Nation to track, gather, and disseminate materials, successes, and lessons learned from the BMAP team's instructor-led courses and site visits.
Link: https://www.dhs.gov/bmap

Insider Threat Video
Discusses how insider threats manifest in a variety of ways including terrorism, workplace violence, and breaches of cybersecurity. The video can be found under the Insider Threat tab.
Link: https://www.dhs.gov/private-citizen

Audience
Type

At-A-Glance Guide For Protecting Faith-Based Venues
Lists the different resources available for houses of worship including security assessments, tabletop exercises, and other training.
Link: https://www.fema.gov/faith-resources

Check It! – Bag Check Video
Provides information facility employees need to properly search bags to protect venues and patrons.
Link: https://www.dhs.gov/video/check-it-bag-check-video

Evacuation Planning Guide for Stadiums
Assists stadium owners and operators with preparing evacuation plans and helping to determine when and how to evacuate, shelter-in-place, or relocate stadium spectators and participants. It also includes a template that can be used to create a plan that will incorporate the unique policies and procedures of state and local governments, surrounding communities, and specific stadium characteristics.

Protective Measures Guides
Provide businesses with an overview of threats and offer suggestions for planning, coordinating, and training activities that contribute to a safe environment for guests and employees. The guides are For Official Use Only (FOUO), but businesses can request access to them through the Commercial Facilities page of the Homeland Security Information Network – Critical Infrastructure (HSIN-CI), which requires registration to access.
- Protective Measures Guide for U.S. Sports Leagues
- Protective Measures Guide for the U.S. Lodging Industry
- Protective Measures Guide for Mountain Resorts
- Protective Measures Guide for Outdoor Venues
- Protective Measures Guide for Commercial Real Estate

Link: https://www.dhs.gov/commercial-facilities-publications

Audience
Type

Protect, Screen, and Allow Access to Facilities
Many large facilities want to screen patrons before allowing them to enter facilities, others may want employ a credentialing process. Resources in this section provide suggestions and guidance on how to put these programs in place.

At-A-Glance Guide For Protecting Faith-Based Venues
Lists the different resources available for houses of worship including security assessments, tabletop exercises, and other training.
Link: https://www.fema.gov/faith-resources

Check It! – Bag Check Video
Provides information facility employees need to properly search bags to protect venues and patrons.
Link: https://www.dhs.gov/video/check-it-bag-check-video

Evacuation Planning Guide for Stadiums
Assists stadium owners and operators with preparing evacuation plans and helping to determine when and how to evacuate, shelter-in-place, or relocate stadium spectators and participants. It also includes a template that can be used to create a plan that will incorporate the unique policies and procedures of state and local governments, surrounding communities, and specific stadium characteristics.

Protective Measures Guides
Provide businesses with an overview of threats and offer suggestions for planning, coordinating, and training activities that contribute to a safe environment for guests and employees. The guides are For Official Use Only (FOUO), but businesses can request access to them through the Commercial Facilities page of the Homeland Security Information Network – Critical Infrastructure (HSIN-CI), which requires registration to access.
- Protective Measures Guide for U.S. Sports Leagues
- Protective Measures Guide for the U.S. Lodging Industry
- Protective Measures Guide for Mountain Resorts
- Protective Measures Guide for Outdoor Venues
- Protective Measures Guide for Commercial Real Estate

Link: https://www.dhs.gov/commercial-facilities-publications

Audience
Type
Sports Venue Bag Search Procedures Guide
Provides suggestions for developing and implementing bag search procedures at venues hosting major sporting events. Venue owners, operators, and event organizers should use additional resources (e.g., consult law enforcement) to implement the procedures outlined in this guide.

Sports Venue Credentialing Guide
Provides suggestions for developing and implementing credentialing procedures at public assembly venues that host professional sporting events. Venue owners, operators, and event organizers should use additional resources (e.g., law enforcement) when available to implement the procedures outlined in this guide.

Patron Screening Best Practices Guide
Provides options for businesses to develop and implement patron screening procedures for major sporting events, concerts, horse races, award ceremonies, and similar gatherings.

Occupant Emergency Programs: An Interagency Security Committee Guide
Provides important information to assist department and agency security planners as they develop and review Occupant Emergency Programs for the safety and security of employees and visitors.

Vehicle-Borne IED Identification and Vehicle Inspection Guidance
Assist stakeholders in identifying suspected vehicle-borne IEDs (VBIED) and provide instruction for vehicle search techniques for use by law enforcement, bomb squads, HAZMAT teams, and other emergency and professional security personnel involved with inspection of vehicles that may pose a terrorist bomb threat. The Vehicle Inspection Guide, Vehicle Inspection Video, and Vehicle-Borne IED Identification Guide are all available to registered users on TRIPwire.
Link: https://tripwire.dhs.gov/IED/appmanager/IEDPortal/IEDDesktop?_nfpb=true&_pageLabel=LOGIN

Interagency Security Committee (ISC) Best Practices for Mail Screening and Handling Processes
Provides mail center managers, their supervisors, and agency security personnel with a framework for understanding and mitigating risks posed to an organization by the mail and packages it receives and delivers on a daily basis.
Link: https://www.dhs.gov/sites/default/files/publications/isc-mail-handling-screening-nonfouo-sept-2012-508.pdf

Crisis Event Response and Recovery Access (CERRA) Framework
Provides voluntary guidance for state, local, tribal, and territorial (SLTT) authorities for planning and developing an access management or program. The framework provides mechanisms, tools, processes, and approaches for coordinating, approving, and enabling access during response and recovery operations.
Protect Against Unmanned Aircraft Systems (UAS)

UAS, also known as drones, can be used to benefit a community by transporting supplies or assisting search and rescue, but they can also be used for malicious purposes. The resources in this section provide an overview of this threat and steps businesses, the public, and first responders can take to protect against the malicious use of drones.

Unmanned Aircraft Systems: Addressing Critical Infrastructure Security Challenges
Provides an overview of the threats posed by UAS and actions that owners and operators can take to protect their facilities.

Audience Type

Unmanned Aircraft Systems: Considerations for Law Enforcement
Provides an overview of UAS and the legal and operational considerations for law enforcement before taking action, and a list of additional resources.

Audience Type

Unmanned Aircraft Systems Frequently Asked Questions
Provides answers to common questions about the requirements and operation of UAS.
Link: https://www.dhs.gov/unmanned-aircraft-systems-faq

Audience Type

Unmanned Aircraft Systems Critical Infrastructure Drone Pocket Card
Provides a quick reference guide for critical infrastructure security and operations officers and the general public on how to identify the different categories of UAS, how to report UAS activity including what information to share, and what actions to take to respond to a threat.

Audience Type

Unmanned Aircraft Systems – Critical Infrastructure Video
Provides information on critical infrastructure challenges associated with the UAS threat, counter-UAS security practices, actions to consider for risk mitigation, and specific preparedness efforts for facilities and organizations. The video can be found under the UAS and Critical Infrastructure – Understanding the Risk tab.
Link: https://www.dhs.gov/uas-ci

Audience Type

Prepare and Respond to Active Assailants
DHS provides a number of resources to help prepare for, and respond to, active assailant incidents, including in-person and online training, tools to prepare emergency action plans, and guidance on the actions to take during an incident.

Active Shooter Preparedness In-Person Workshops
Features scenario-based workshops with facilitated discussions to engage private sector professionals and law enforcement representatives from federal, state, and local agencies to learn how to prepare for, and respond to, an active shooter situation. Through the course of the exercises, participants evaluate current response concepts, plans, and capabilities for coordinated responses to active shooter incidents.
Link: https://www.dhs.gov/active-shooter-workshop-participant

Audience Type
**Active Shooter Preparedness Resource Materials**

Assist businesses, government offices, and schools in preparing for, and responding to, an active shooter. These resources are also available in the following languages: Arabic, Chinese, Korean, Punjabi, Russian, Somali, Spanish, and Urdu.

- **Active Shooter Booklet**: provides information on how to respond to an active shooter in your vicinity, how to react when law enforcement arrives, and how to train staff and prepare for an active shooter situation, including roles and responsibilities.
  
  Link: https://www.dhs.gov/xlibrary/assets/active_shooter_booklet.pdf

- **Active Shooter Event Quick Reference Guide**: provides key information in a shorter, easy-to-read format.
  

- **Active Shooter Poster**: highlights key information for how to respond when an active shooter is in your vicinity.
  

- **Active Shooter Pocket Card**: contains all the information needed to respond to an active shooter in an accessible format.
  

- **Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practices Guide**: includes helpful information and best practices for federal agencies that can be applied more broadly by anyone who may be involved in an active shooter situation.
  

- **Options for Consideration Active Shooter Preparedness Video**: demonstrates possible actions to take if confronted with an active shooter scenario. The video also shows how to assist authorities once law enforcement enters the scene.
  
  Link: https://www.dhs.gov/options-consideration-active-shooter-preparedness-video

**Active Shooter Preparedness Program Website**

Provides access to a number of DHS products, tools, and resources to help everyone prepare for and respond to an active shooter incident.

Link: https://www.dhs.gov/active-shooter-preparedness

**Active Shooter Recovery Materials**

Help organizations proactively put in place policies and procedures to help effectively recover from an active shooter incident while providing a support structure for all involved.

- **Active Shooter Recovery Guide**: outlines what to do in the short-term and long-term to aid in recovery.
  

- **Recovering From An Active Shooter Incident Action Guide**: provides information on how to establish a recovery process and breaks down necessary actions for short-term and long-term recovery following an active shooter incident.
  

**Vehicle Ramming Attack Mitigation Video**

Provides information to assist in mitigating the threat of vehicle ramming attacks with technical analysis from public and private sector subject matter experts. The video leverages real-world events, and provides recommendations aimed at protecting organizations as well as individuals against a potential vehicle ramming incident.

Link: https://www.dhs.gov/private-citizen
Active Shooter Emergency Action Planning

Describes the fundamental concepts of developing an Emergency Action Planning (EAP) for an active shooter scenario, including important consideration of EAP development.

- **Video**: guides viewers through important considerations of EAP development through the first-hand perspectives of active shooter survivors, first responder personnel, and other subject matter experts who share their unique insight.
  Link: https://www.dhs.gov/active-shooter-emergency-action-plan-video

- **Guide**: provides the information needed to develop an Emergency Action Plan.

- **Template**: provides the framework for businesses to create their own Emergency Action Plan.

**Audience**

**Type**

---

Prevent and Respond to Bombings

The resources in this section are designed to increase the capabilities of everyone—the public, business owners and staff, government employees, law enforcement, and first responders—to prevent, protect against, and respond to bombing incidents. The resources include an easy-to-use checklist, planning assistance, in-person and online training, materials and videos that provide guidance, and an online network to access additional resources and share information.

**What to Do – Bomb Threat Website**

Provides guidance and resources including in-depth procedures for responding to bomb threats or encounters with suspicious items or behaviors and provides information to help prepare and react appropriately during these events. The Website also provides information regarding other planning and preparedness resources.

Link: https://www.dhs.gov/what-to-do-bomb-threat

- **DHS-DOJ Bomb Threat Guidance**: provides detailed information on how to assess and react to a threat.

- **Bomb Threat Procedures Checklist**: provides basic procedural guidelines and a checklist to document important information if a bomb threat is received.
  Link: https://tripwire.dhs.gov/IED/resources/docs/DHS%20Bomb%20Threat%20Checklist.pdf

- **What You Can Do When There is a Bomb Threat Video**: demonstrates how to specifically respond to a phoned in bomb threat and was developed in partnership with the University of Central Florida and the International Association of Chiefs of Police (IACP).
  Link: https://www.dhs.gov/what-to-do-bomb-threat

- **Bombing Prevention Lanyard Cards**: provide quick-reference information and key reminders to empower action, both on the job every day and in the event of an incident.

**Audience**

**Type**
Technical Resource for Incident Prevention (TRIPwire) Website
Serves as a 24/7 online, collaborative information-sharing network for bomb squads, first responders, military personnel, government officials, intelligence analysts, and security professionals. Developed and maintained by the Office for Bombing Prevention (OBP), TRIPwire combines expert analyses and reports with relevant documents, images, and videos gathered directly from terrorist source materials to help users anticipate, identify, and prevent IED incidents. TRIPwire requires registration to access information, or partners can log-in using their HSIN account. To login, please visit: https://tripwire.dhs.gov/IED/appmanager/IEDPortal/IEDDesktop?_nfpb=true&_pageLabel=LOGIN
Overview Video: https://tripwire.dhs.gov/IED/resources/jsp/tripwireVideo.jsp

Sports and Entertainment Venues Bombing Prevention Solutions Portfolio
Provides information on and direct access to the trainings, products, and resources that support sports and entertainment organizations and venues with building counter-IED capabilities. The interactive product connects leadership within these organizations to the counter-IED resources that meet their needs, and empowers all venue personnel to play a role in security.

Multi-Jurisdictional Improvised Explosive Device Security Planning (MJIEDSP) Program
Assists communities with collectively identifying roles, responsibilities, and capability gaps; and optimizing limited resources within a multi-jurisdictional planning area. The MJIEDSP process includes coordination with stakeholders in an area to conduct familiarization briefs and training, data collection activities, and facilitated scenario-based workshops.
Link: https://www.dhs.gov/mjiedsp

Counter-IED and Risk Mitigation Training
Provides participants—including municipal officials and emergency managers, state and local law enforcement and other emergency services, critical infrastructure owners and operators, and professional security personnel—with general information and strategies to prevent, protect against, respond to, and mitigate bombing incidents.
To request direct delivery trainings, please contact your local Protective Security Advisor (PSA) or email OBP@hq.dhs.gov for additional information. For more information, or for a full list of Counter-IED and Risk Mitigation trainings, visit the Counter-IED Training Courses Website or the Counter-IED & Risk Mitigation Training Factsheet.
Link: https://www.dhs.gov/bombing-prevention-training-courses

“I think you saved my life. ... I was so thankful I knew what to do.”
– Hailey Harris of Cambridge, MA; Boston Marathon bombing survivor and beneficiary of OBP counter-IED training
Connect with the Office of Infrastructure Protection

This section lists ways that businesses; first responders; and state, local, tribal, and territorial governments can access not only the resources listed in this guide, but additional resources available through IP. These resources can help identify the tools, resources, and training that are right for each facility and its risks.

National Infrastructure Coordinating Center (NICC)
Serves as the dedicated 24/7 coordination and information sharing operations center that maintains situational awareness of the Nation’s critical infrastructure. For more information, please email NICC@hq.dhs.gov.

Link: https://www.dhs.gov/national-infrastructure-coordinating-center

IP Regional Offices
Engage with state, local, tribal, and territorial (SLTT) government partners, businesses, and critical infrastructure owners and operators in their regions to provide access to steady-state DHS risk-mitigation tools, products, and services, such as training and voluntary vulnerability assessment programs.

The 10 IP Regional Offices also support National Special Security Events (NSSEs) and Special Event Assessment Rating (SEAR) events; support response to all-hazard incidents through field-level coordination and information sharing; and provide expertise on reconstituting affected critical infrastructure.

- IP Regional Office Website: https://www.dhs.gov/ip-regional-offices

Homeland Security Information Network – Critical Infrastructure (HSIN-CI)
Serves as the primary information-sharing platform between the critical infrastructure sector stakeholders and government. HSIN-CI enables federal, state, local, and private sector critical infrastructure owners and operators to communicate, coordinate, and share sensitive and sector-relevant information to protect their critical assets, systems, functions, and networks at no charge to sector stakeholders. To request access to HSIN-CI, please contact hsinci@hq.dhs.gov.

Link: https://www.dhs.gov/hsin-critical-infrastructure

Interagency Security Committee (ISC)
Develops policies, standards, and recommendations related to the security of nonmilitary federal facilities across the Nation. The ISC does this by, with, and through its members.

Link: https://www.dhs.gov/about-interagency-security-committee

Assist Visits and the Infrastructure Survey Tool
Informs critical infrastructure owners and operators of the importance of their facilities, how they fit into the broader critical infrastructure sector, and provides an overview of the IP resources available to help enhance security and resilience. The visits, conducted by PSAs with critical infrastructure facility representatives, help build relationships and increase communications. One of the IP resources available to facility owners and operators is the Infrastructure Survey Tool (IST).

Assist visits: https://www.dhs.gov/assist-visits
Infrastructure Survey Tool: https://www.dhs.gov/infrastructure-survey-tool
# Contacts

## Key Contacts

<table>
<thead>
<tr>
<th>AGENCY/DIVISION/PROGRAM</th>
<th>PHONE/EMAIL</th>
<th>WEBSITE</th>
<th>INFORMATION PROVIDED</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Infrastructure Coordinating Center</td>
<td><a href="mailto:NICC@hq.dhs.gov">NICC@hq.dhs.gov</a></td>
<td><a href="https://dhs.gov/national-infrastructure-coordinating-center">https://dhs.gov/national-infrastructure-coordinating-center</a></td>
<td>For more information about the NICC</td>
</tr>
<tr>
<td>IP Regional Offices</td>
<td>Please see Website for contact information</td>
<td><a href="https://www.dhs.gov/ip-regional-offices">https://www.dhs.gov/ip-regional-offices</a></td>
<td>For more information on the IP Regional Offices, including locations, services, and contact information for each region</td>
</tr>
</tbody>
</table>

## Additional Contacts

<table>
<thead>
<tr>
<th>AGENCY/DIVISION/PROGRAM</th>
<th>PHONE/EMAIL</th>
<th>WEBSITE</th>
<th>INFORMATION PROVIDED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Shooter Preparedness Program</td>
<td><a href="mailto:ASworkshop@hq.dhs.gov">ASworkshop@hq.dhs.gov</a></td>
<td><a href="https://www.dhs.gov/active-shooter-preparedness">https://www.dhs.gov/active-shooter-preparedness</a></td>
<td>For information on Active Shooter Preparedness workshops and materials</td>
</tr>
<tr>
<td>Commercial Facilities Sector-Specific Agency</td>
<td><a href="mailto:CFSteam@hq.dhs.gov">CFSteam@hq.dhs.gov</a></td>
<td><a href="https://www.dhs.gov/commercial-facilities-sector">https://www.dhs.gov/commercial-facilities-sector</a></td>
<td>For more information on available DHS resources</td>
</tr>
<tr>
<td>Homeland Security Information Network – Critical Infrastructure</td>
<td><a href="mailto:hsinci@hq.dhs.gov">hsinci@hq.dhs.gov</a></td>
<td><a href="https://www.dhs.gov/hsin-critical-infrastructure">https://www.dhs.gov/hsin-critical-infrastructure</a></td>
<td>To request access to HSIN-CI include the following information: name, company, official email address, supervisor’s name and phone number, and critical infrastructure sector</td>
</tr>
<tr>
<td>Interagency Security Committee</td>
<td><a href="mailto:isc.dhs.gov@hq.dhs.gov">isc.dhs.gov@hq.dhs.gov</a></td>
<td><a href="https://www.dhs.gov/interagency-security-committee">https://www.dhs.gov/interagency-security-committee</a></td>
<td>For more information on policies, standards, and best practices that can be applied</td>
</tr>
<tr>
<td>Office for Bombing Prevention</td>
<td><a href="mailto:OBP@hq.dhs.gov">OBP@hq.dhs.gov</a></td>
<td><a href="https://www.dhs.gov/obp">https://www.dhs.gov/obp</a></td>
<td>For more information on resources or to request training</td>
</tr>
<tr>
<td>Soft Target Security Program</td>
<td><a href="mailto:IP-softtargetsecurity@hq.dhs.gov">IP-softtargetsecurity@hq.dhs.gov</a></td>
<td><a href="https://www.dhs.gov/soft-target-security">https://www.dhs.gov/soft-target-security</a></td>
<td>For more information on soft target security resources</td>
</tr>
<tr>
<td>TRIPwire Help Desk</td>
<td>1-866-987-9473; <a href="mailto:TRIPwirehelp@hq.dhs.gov">TRIPwirehelp@hq.dhs.gov</a></td>
<td><a href="https://tripwire.dhs.gov">https://tripwire.dhs.gov</a></td>
<td>TRIPwire is available at no cost to registered subscribers and now also features a public-access homepage with valuable preparedness information for the whole community</td>
</tr>
<tr>
<td>Unmanned Aircraft Systems Program</td>
<td><a href="mailto:IP-UAS@hq.dhs.gov">IP-UAS@hq.dhs.gov</a></td>
<td><a href="https://www.dhs.gov/uas-ci">https://www.dhs.gov/uas-ci</a></td>
<td>For information on UAS resources</td>
</tr>
</tbody>
</table>