



UNCLASSIFIED

ATTENTION—SURFACE TRANSPORTATION STAKEHOLDERS

(U) The Transportation Security Administration (TSA) is providing this Security Awareness Message (SAM) to our industry partners in light of the upcoming Memorial Day weekend when large numbers of travelers will be taking to the roads, rails, and skies. This document is not issued in response to a specific threat to the Nation.

(U) The [National Terrorism Advisory System](#) Bulletin reissued May 9, 2018, highlights the continuing threat posed by homegrown terrorists who use readily available tactics and weapons such as improvised explosive devices, vehicle ramming, small arms, and edged weapons. At present, the TSA Office of Intelligence and Analysis is not aware of information to suggest any imminent plots against the United States' surface transportation modes. However, the potential remains for individuals, who are radicalized or otherwise motivated to violence, to attack the nation's transportation systems.

(U) TSA remains concerned about attacks perpetrated by homegrown violent extremists and lone offenders in the Homeland and abroad, particularly in places where crowds gather. In light of the attractiveness of such soft targets, TSA encourages our industry partners to review the [“Security of Soft Targets and Crowded Places-Resource Guide”](#) from the Department of Homeland Security's Office of Infrastructure Protection for tools and training to enhance the security of these locations.

(U) TSA encourages transportation stakeholders to report suspicious activity in accordance with their company's or agency's security plan. Persons whose behavior does not fit their circumstances or surroundings should be brought to the attention of law enforcement. Contact information for company supervisors, local law enforcement, and [the local FBI field office](#) should be readily available to employees to assist them in reporting suspicious activity.

(U) For mass transit and passenger rail operators, [Operation RAILSAFE](#) is scheduled for May 24, 2018. Law enforcement agencies are encouraged to increase security at transit stations, railroad stations, and rights-of-way. If eligible under program guidance, transit and passenger rail systems that have received funding through the Transit Security Grant Program may reprogram funds to cover costs associated with implementing the actions recommended in this message, including operational overtime expenses, for the period May 23-29, 2018.

Sonya T. Proctor
Director, Surface Division
Office of Security Policy and Industry Engagement
Transportation Security Administration
Department of Homeland Security





Homeland
Security



National Protection and Programs Directorate
Office of Infrastructure Protection

Security of Soft Targets and Crowded Places—Resource Guide

April 2018

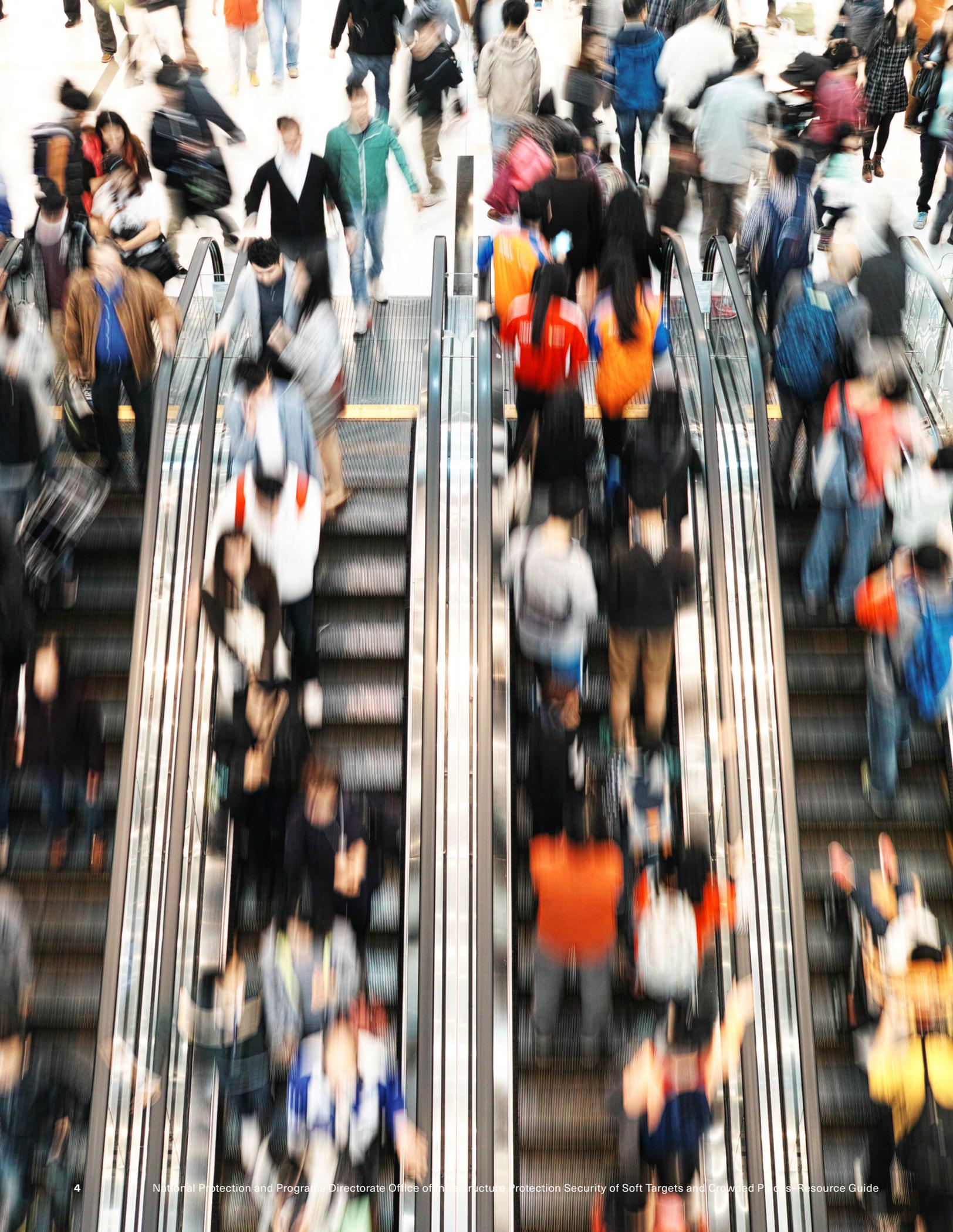


Table of Contents

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

- 2 Resource Descriptions & Links** 9
 - 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



For Everyone

CATEGORY	RESOURCE	TYPE
Understand the Basics	Tools and Resources to Help Businesses Plan, Prepare, and Protect from an Attack	
	"If You See Something, Say Something" Campaign® Informational Video and Radio PSA	
	"If You See Something, Say Something" Campaign® Informational Print Materials PSA	
Identify Suspicious Behavior	Insider Threat Video	
	Pathway to Violence Action Guide	
	Pathway to Violence Video	
	What's in Store: Ordinary People, Extraordinary Events Video	
Protect Against Unmanned Aircraft Systems	Unmanned Aircraft Systems (UAS) Critical Infrastructure Drone Pocket Card	
	UAS Frequently Asked Questions	
	Active Shooter Booklet	
	Active Shooter Preparedness Program Website	
	Active Shooter Event Quick Reference Guide	
Prepare and Respond to Active Assailants	Active Shooter Poster	
	Active Shooter Pocket Card	
	Options for Consideration Active Shooter Preparedness Video	
	Vehicle Ramming Attack Mitigation Video	

Legend: Type of Resource



Fact Sheet



Guide



Informational Materials



In-Person Training



Online Training



Tool



Video



Website



For **Businesses**

CATEGORY	RESOURCE	TYPE
Understand the Basics	Business Continuity Planning Suite	
	Independent Study Training Courses	
	Sector-Specific Tabletop Exercise Program (SSTEP)	
Identify Suspicious Behavior	Bomb-Making Materials Awareness Program (BMAP)	
	Nationwide Suspicious Activity Reporting (SAR) Initiative – Private Sector Security	
	No Reservations: Suspicious Behavior in Hotels Video	
Protect, Screen, and Allow Access to Facilities	Suspicious Behavior Advisory Posters	
	At-A-Glance Guide for Protecting Faith-Based Venues	
	Check It! – Bag Check Video	
	Evacuation Planning Guide for Stadiums	
	Patron Screening Best Practices Guide	
	Protective Measures Guides	
	Sports Venue Bag Search Procedures Guide	
	Sports Venue Credentialing Guide	
	Vehicle-Borne Improvised Explosive Device (IED) Identification Guide	
	Vehicle Inspection Guide	
Vehicle Inspection Video		
Protect Against Unmanned Aircraft Systems	Unmanned Aircraft Systems: Addressing Critical Infrastructure Security Challenges	
	Unmanned Aircraft Systems – Critical Infrastructure Video	
Prepare and Respond to Active Assailants	Active Shooter Preparedness In-Person Workshops	
	Active Shooter Emergency Action Planning Guide	
	Active Shooter Emergency Action Planning Template	
	Active Shooter Emergency Action Planning Video	
	Active Shooter Recovery Guide	
Recovering From An Active Shooter Incident Action Guide		

Legend: Type of Resource



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

For Government

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

For First Responders

CATEGORY	RESOURCE	TYPE
Protect, Screen, and Allow Access to Facilities	Crisis Event Response and Recovery Access (CERRA) Framework	
Protect Against Unmanned Aircraft Systems	Unmanned Aircraft Systems: Considerations for Law Enforcement	



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/sites/default/files/publications/Hometown-Security-Fact-Sheet-04062016-508.pdf>

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

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 

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 

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.

Nationwide Suspicious Activity Reporting (SAR) Initiative – Private Sector Security Training

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.

Link: <https://nsi.ncirc.gov/hsptregistration/private-sector/>

Audience  Type 

No Reservations: Suspicious Behavior in Hotels Video

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.

Link: <https://www.dhs.gov/video/no-reservations-suspicious-behavior-hotels>

Audience  Type 

“If You See Something, Say Something” Campaign®

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.

Link: <https://www.dhs.gov/see-something-say-something/campaign-materials>

Audience  Type  

Pathway to Violence Action Guide

Explains warning signs that may lead to violence and what individuals can do to mitigate a potential incident.

Link: <https://www.dhs.gov/sites/default/files/publications/dhs-pathway-to-violence-09-15-16-508.pdf>

Audience  Type 

Pathway to Violence Video

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.

Link: <https://www.dhs.gov/pathway-violence-video>

Audience  Type 

Suspicious Behavior Advisory Posters

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.

Link: <https://tripwire.dhs.gov/IED/resources/jsp/loginPopup2.jsp>

Audience   Type 

What's in Store: Ordinary People, Extraordinary Events Video

Helps owners, managers, and staff at shopping centers and retail establishments identify and report suspicious activity and threats by highlighting the indicators of suspicious activity in retail settings.

Link: <https://www.dhs.gov/video/whats-store-ordinary-people-extraordinary-events>

Audience  Type 

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 

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>

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>

Audience 

Type 

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>

Audience 

Type 

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.

Link: <https://www.dhs.gov/sites/default/files/publications/evacuation-planning-guide-stadiums-508.pdf>

Audience 

Type 

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.

Link: <https://www.dhs.gov/sites/default/files/publications/sports-venue-bag-search-guide-508.pdf>

Audience   Type 

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.

Link: <https://www.dhs.gov/sites/default/files/publications/sports-venue-credentialing-guide-508.pdf>

Audience  Type 

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.

Link: <https://www.dhs.gov/sites/default/files/publications/patron-screening-guide-03-16-508.pdf>

Audience   Type 

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.

Link: <https://www.dhs.gov/sites/default/files/publications/isc-occupant-emergency-programs-guide-mar-2013-508.pdf>

Audience  Type 

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

Audience   Type  

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>

Audience  Type 

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.

Link: <https://www.dhs.gov/sites/default/files/publications/Crisis%20Event%20Response%20and%20Recovery%20Access%20%28CERRA%29%20Framework.pdf>

Audience    Type 

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.

Link: <https://www.dhs.gov/sites/default/files/publications/uas-ci-challenges-fact-sheet-508.pdf>

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.

Link: <https://www.dhs.gov/sites/default/files/publications/uas-law-enforcement-considerations-508.pdf>

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.

Link: <https://www.dhs.gov/sites/default/files/publications/uas-ci-drone-pocket-card-112017-508.pdf>

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.
Link: <https://www.dhs.gov/sites/default/files/publications/active-shooter-pamphlet-2017-508.pdf>
- **Active Shooter Poster:** highlights key information for how to respond when an active shooter is in your vicinity.
Link: <https://www.dhs.gov/sites/default/files/publications/active-shooter-poster-2017-508.pdf>
- **Active Shooter Pocket Card:** contains all the information needed to respond to an active shooter in an accessible format.
Link: <https://www.dhs.gov/sites/default/files/publications/active-shooter-pocket-card-508.pdf>
- **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.
Link: <https://www.dhs.gov/sites/default/files/publications/isc-planning-response-active-shooter-guide-non-fouo-nov-2015-508.pdf>
- **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>

Audience  Type   

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>

Audience  Type 

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.
Link: <https://www.dhs.gov/sites/default/files/publications/active-shooter-recovery-guide-08-08-2017-508.pdf>
- **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.
Link: <https://www.dhs.gov/sites/default/files/publications/recovering-from-an-active-shooter-incident-fact-sheet-08-08-2017-508.pdf>

Audience  Type  

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>

Audience  Type 

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.
Link: <https://www.dhs.gov/sites/default/files/publications/active-shooter-emergency-action-plan-112017-508v2.pdf>
- **Template:** provides the framework for businesses to create their own Emergency Action Plan.
Link: <https://www.dhs.gov/sites/default/files/publications/active-shooter-emergency-action-plan-template-112017-508.pdf>

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.
Link: https://tripwire.dhs.gov/IED/resources/docs/OBP_DHS_DOJ_Bomb_Threat_Guidance.pdf
- **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.
Link: [https://tripwire.dhs.gov/IED/resources/docs/Bombing%20Prevention%20Lanyard%20Cards%20\(Lined%20Version\).pdf](https://tripwire.dhs.gov/IED/resources/docs/Bombing%20Prevention%20Lanyard%20Cards%20(Lined%20Version).pdf)

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

Link: <https://www.dhs.gov/sites/default/files/publications/obp-tripwire-fact-sheet-2016-508.pdf>

Overview Video: <https://tripwire.dhs.gov/IED/resources/jsp/tripwireVideo.jsp>

Audience    Type   

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.

Link: <https://tripwire.dhs.gov/IED/resources/docs/Sports%20Entertainment%20Venue%20Bombing%20Prevention%20Solutions%20Portfolio.pdf>

Audience   Type     

“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

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>

Audience    Type  

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>

Fact sheet: <https://www.dhs.gov/sites/default/files/publications/obp-training-fact-sheet-2017-508.pdf>

Audience   Type   

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>

Audience   Type  

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 Fact Sheet: <https://www.dhs.gov/sites/default/files/publications/IP-Regional-Enhancement-Fact-Sheet-508-F.pdf>
- IP Regional Office Website: <https://www.dhs.gov/ip-regional-offices>
- Protective Security Advisor (PSA) Program Fact Sheet: <https://www.dhs.gov/sites/default/files/publications/PSA-Program-Fact-Sheet-05-15-508.pdf>

Audience    Type   

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>

Audience   Type 

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>

Audience  Type 

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>

Audience  Type  



3 Contacts

KEY CONTACTS			
AGENCY/DIVISION/PROGRAM	PHONE/EMAIL	WEBSITE	INFORMATION PROVIDED
National Infrastructure Coordinating Center	NICC@hq.dhs.gov	https://dhs.gov/national-infrastructure-coordinating-center	For more information about the NICC
IP Regional Offices	Please see Website for contact information	https://www.dhs.gov/ip-regional-offices	For more information on the IP Regional Offices, including locations, services, and contact information for each region
ADDITIONAL CONTACTS			
AGENCY/DIVISION/PROGRAM	PHONE/EMAIL	WEBSITE	INFORMATION PROVIDED
Active Shooter Preparedness Program	ASworkshop@hq.dhs.gov	https://www.dhs.gov/active-shooter-preparedness	For information on Active Shooter Preparedness workshops and materials
Commercial Facilities Sector-Specific Agency	CFSteam@hq.dhs.gov	https://www.dhs.gov/commercial-facilities-sector	For more information on available DHS resources
Homeland Security Information Network – Critical Infrastructure	hsinci@hq.dhs.gov	https://www.dhs.gov/hsin-critical-infrastructure	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
Interagency Security Committee	isc.dhs.gov@hq.dhs.gov	https://www.dhs.gov/interagency-security-committee	For more information on policies, standards, and best practices that can be applied
Office for Bombing Prevention	OBP@hq.dhs.gov	https://www.dhs.gov/obp	For more information on resources or to request training
Soft Target Security Program	IP-softtargetsecurity@hq.dhs.gov	https://www.dhs.gov/soft-target-security	For more information on soft target security resources
TRIPwire Help Desk	1-866-987-9473; TRIPwirehelp@dhs.gov	https://tripwire.dhs.gov	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
Unmanned Aircraft Systems Program	IP-UAS@hq.dhs.gov	https://www.dhs.gov/uas-ci	For information on UAS resources



Homeland
Security

U.S. Department of Homeland Security
National Protection and Programs Directorate
Office of Infrastructure Protection
Washington, D.C. 20528