



VENUE GUIDE FOR SECURITY ENHANCEMENTS

JANUARY 2025

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

CONTENTS

Background and Content	1
The Model.....	1
Purpose	2
Scope	2
Risk Assessment	3
Security Measures.....	3
Cost Levels.....	3
Complexity Levels.....	3
Security Enhancements Table	4
Coordination and Administration.....	4
Installation of Security Measure.....	5
Train and Exercise.....	6
Perimeter Security.....	7
Access Control.....	7
Crowd Management.....	8
Traffic Management.....	8
Emergency Management.....	8
Glossary	9
Resources	10



BACKGROUND AND CONTENT

As the Sector Risk Management Agency for Commercial Facilities, the Cybersecurity and Infrastructure Security Agency (CISA) is committed to partnering with venue operators in mitigating the threat of targeted violence and preparing for potential incidents. In collaboration with industry experts and security professionals, CISA developed the *Venue Guide for Security Enhancements*. Applying the guide will enable venue operators to effectively identify and manage risk.

This guide serves as a broad catalog to support safe and secure day-to-day operations and event management planning and execution. Use of the guidance in this resource will not deter or prevent all threats. As appropriate, venues should have response and recovery plans. However, because every venue is unique, CISA recommends conducting a site-specific physical security assessment.

THE MODEL

The ‘Security Enhancements Table’ within this guide is a model to help operators understand the security measure options, intended outcomes, risks addressed, and benchmarks for robust security practices. For additional information and context, please see the Glossary and Resources sections located at the end of the document.

The *Venue Guide for Security Enhancements* is:

- **Voluntary:** The security measures outlined in this guide are optional considerations to enhance security posture and risk tolerance, but they do not place any obligation on venue operators. This information can and should be tailored to the needs of each individual venue.
- **Not Comprehensive:** The guide offers a core set of security considerations and mitigations that are broadly applicable, but it does not identify all physical security considerations needed for venue operators. Before implementing, consider the type of venue and the unique challenges it faces and create a personalized risk management strategy.

DISCLAIMER: The approaches, techniques, and tactics described in this Guide are not intended to mandate policy or direct any action. This document is not intended to, and does not, create any legal rights, nor does it provide any defense against civil or criminal liability.

PURPOSE

This guide aims to help venue operators enhance safety, protect assets, and create secure environments through effective security measures and best practices. The guide:

1. **Provides guidance for venues**, such as evaluating security measures, complexity levels, costs, options, and threats mitigated by these measures. By balancing these factors, venues can create a secure environment for operators and guests.
2. **Recommends broadly applicable considerations for evaluating security practices**, such as assessing measures and improving physical security compliance to ensure staff and visitor safety.
3. **Offers actionable guidance** for prioritizing the most effective security practices and proactively reducing the risk of major threats.
4. **Provides venue operators with a tailored menu of security options**, allowing them to select the most suitable and effective measures for their venue's budget, size, location, and risk factors.

Venue operators have access to a range of cyber and physical services through CISA online and in person. Reach out to your local CISA advisors by finding your region [here](#).

SCOPE

This guide outlines physical security considerations at venues and special events. These guidelines help conduct risk assessment analysis to identify and address security vulnerabilities. Reviewing and applying these security considerations will help venue operators to become proactive and meet physical security expectations.

RISK ASSESSMENT

To ensure the safety of staff and venue guests, venue operators should conduct a thorough risk assessment to properly identify and mitigate potential threats. Operators can then use the table below and, keeping in mind **venue complexity** and **budgetary constraints**, identify **security measures** that would cover the gaps in established security strategies.

SECURITY MEASURES

Security measures are crucial for venue operators to maintain safety and order. This involves implementing fencing, lighting, access control, and surveillance systems to secure the venue's boundaries. It also includes crowd management techniques such as employing barriers and training staff to ensure effective crowd control during events or gatherings.

The measures in the table below were developed in coordination with CISA subject matter experts using the sources listed in the Resources section.

These measures prevent unauthorized access to sensitive areas and enhance security within the venue. Overall, these security measures work in tandem to create a safe and secure space for venue activities.

For implementing security measures at a venue, cost levels will vary depending on factors such as jurisdiction, budget, risk assessment results, resource availability, threat landscape, and industry laws and regulations.

COST LEVELS

The table also displays a general estimate with dollar symbols (\$) for implementing the security measures that will differ depending on the venue's available resources.

\$: Security measures that require little to no funding to implement. Measures at this level include training screening staff on proper search procedures, posting signs of prohibited items, or marking entry and exit points.

\$\$: Security measures that require moderate funding increases and are more difficult to implement. Measures at this level include providing photo IDs for staff, conducting evacuation drills, or minimizing shrubbery around access points.

\$\$\$: Security measures that require a high level of funding and potentially significant financial investment from outside sources. Measures at this level include implementing crime prevention landscaping, installing site-wide video surveillance systems, or acquiring and employing advanced cybersecurity systems.

COMPLEXITY LEVELS

The table displays a given measure's complexity level to help operators determine whether it is easy to implement or if more substantial resources are required. Resources may include staff, systems, equipment, or capital. These complexity levels are a general estimate and are dependent on the individual venue. **However, complexity does not equal effectiveness and will vary based on the specific venue.**

Low: Security measures that are easy to implement using readily available resources, such as training existing staff members, upgrading the current basic systems, using easily accessible and affordable equipment, or allocating capital for security measures with a low impact to the venue's budget.

Moderate: Security measures requiring resources that are not readily available but possibly accessible with increased effort, such as hiring additional staff with unique expertise, acquiring new systems or technologies, investing in equipment upgrades, or allocating moderate capital to support security initiatives.

High: Security measures requiring resources that are not readily available and involve significant effort to obtain, such as hiring specialized security personnel or consultants, acquiring advanced security systems or equipment exceeding the current budget, extensive training, long-term construction projects, or allocating substantial capital to support security initiatives.



In the table below, security measures are presented as sections of a basic security plan. The presence of a shield indicates that the identified measure is effective at mitigating that threat. If there is no shield present, the measure is not effective against that threat.

SECURITY ENHANCEMENTS TABLE

Security Measure Options

(numbers refer to relevant entries in Resources section)

	Cost Level	Complexity Level	Threats Mitigated by Security Measure														
			Active Shooter	Vehicle Incident	Improvised Explosive Device (IED)	Vehicle-Borne IED (VBIED)	Crowd Control	Chem/Bio WMD	Hostile Patrons	Civil Disturbance	Unmanned Aircraft Systems	Loss of Services/Disruption	Industrial Incident	Natural Disaster/Extreme Weather [Event]	Event Cancellation*	Theft/Vandalism*	
Develop procedures for patrons with access and functional needs ^{3, 6, 8}	\$	Low	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Verify procedures are established in the EAP for sheltering/evacuation ^{6, 11, 18}	\$	Low	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Schedule fire, EMS, and law enforcement to tour venue/hold training events ^{6, 8, 17, 18, 19}	\$	Low	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Establish pre-set emergency communications plans with decision points ^{5, 6, 8, 10, 16, 17}	\$	Low	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Establish procedures to ensure only authorized personnel and vehicles can enter specified restricted areas ^{6, 13, 17}	\$	Low	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Establish emergency communication procedures for patrons with functional needs ^{6, 8, 10, 17, 18}	\$	Low	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Develop and post entry requirements (clear bag policy, bag size restrictions) and prohibited items ^{12, 13, 14, 17}	\$	Low	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Develop traffic flow patterns ^{23, 24}	\$	Low	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Designate drop-off areas for handicapped or other designated personnel ^{23, 24}	\$	Low	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Establish safe handling procedures for responding to downed UAS ^{2, 20}	\$	Low	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Develop an Event-Specific Occupancy Plan ^{4, 5, 6, 8, 11, 16, 17, 18}	\$	Low	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Designate drop-off areas for ride-share ^{23, 24}	\$	Low	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

*** DISCLAIMER:** Issues regarding theft, vandalism, and event cancellation would be handled, if necessary, by state and local officials. The information is included here only to note that they are threats that some venues should need to consider.

Security Measure Options

(numbers refer to relevant entries in Resources section)

	Cost Level	Complexity Level	Threats Mitigated by Security Measure													Event Cancellation*	Theft/Vandalism*
			Active Shooter	Vehicle Incident	Improvised Explosive Device (IED)	Vehicle-Borne IED (VBIED)	Crowd Control	Chem/Bio WMD	Hostile Patrons	Civil Disturbance	Unmanned Aircraft Systems	Loss of Services/Disruption	Industrial Incident	Natural Disaster/Extreme Weather [Event]			
Coordination and Administration (cont.)																	
Acquire City/County or local permit for venue ^{6, 8, 17, 18, 19}	\$	Low															
Develop Incident Response Plans as part of the EAP for each specific emergency response (Active Shooter, Bomb threat, etc.) ^{1, 6, 7, 8, 11, 15, 18, 20}	\$	Mod.															
Establish plans with local, state, and federal response agencies ^{4, 6, 17, 19}	\$	High															
Complete a risk assessment or security survey of the venue ^{5, 6, 16, 18}	\$\$	Mod.															
Develop a Venue Emergency Action Plan (EAP) ^{6, 8, 17, 18}	\$\$	Mod.															
Develop a Traffic Management Plan with the Crowd Management Plan and mitigate hostile vehicle threat areas ^{22, 23, 24}	\$\$	Mod.															
Coordinate food waste pickup procedures ^{6, 8}	\$\$	Mod.															
Establish a Crime Prevention Through Environmental Design (CPTED) Strategy ^{5, 6, 8, 11, 17, 18}	\$\$	High															
Utilize bomb squad and explosives detection canine team(s) for event screening ^{3, 4, 5, 6, 8, 13, 20}	\$\$\$	High															
Installation of Security Measure																	
Refer to the Primary, Alternate, Contingency, Emergency (PACE) communications ecosystem for installing radio, cellular, and communication systems with back-ups and rapid recovery plans that are frequently tested ^{8, 10}	\$\$	Mod.															
Install security systems for HVAC, mechanical, gas, fuel, and drainage systems ^{8, 10}	\$\$	Mod.															
Install fencing for traffic, crowd control, and security ^{6, 8}	\$\$\$	Mod.															
Install a Video Surveillance System (VSS) to assist with crowd control/monitoring ^{6, 8}	\$\$\$	High															

Security Measure Options

(numbers refer to relevant entries in Resources section)

	Cost Level	Complexity Level	Threats Mitigated by Security Measure													
			Active Shooter	Vehicle Incident	Improvised Explosive Device (IED)	Vehicle-Borne IED (VBIED)	Crowd Control	Chem/Bio WMD	Hostile Patrons	Civil Disturbance	Unmanned Aircraft Systems	Loss of Services/Disruption	Industrial Incident	Natural Disaster/Extreme Weather [Event]	Event Cancellation*	Theft/Vandalism*
Installation of Security Measure (cont.)																
Install adequate lighting for critical areas such as evacuation points ^{6, 8}	\$\$\$	High	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
Install adequate lighting in parking areas ^{6, 8}	\$\$\$	High	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓		✓	✓
Install adequate LED lighting to assist with visual aid and camera surveillance ^{6, 8}	\$\$\$	High	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓		✓	✓
Consider using UAS detection, tracking, identification (DTI) technology, Remote ID receivers, and/or configuring CCTV cameras to monitor for aerial threats ^{2, 21}	\$\$\$	High			✓	✓		✓		✓	✓	✓				
Train and Exercise																
Train/inform screening staff on safety actions to take in accordance with the EAP ^{6, 13}	\$	Low	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Train staff on code of conduct, acceptable and unacceptable patron behaviors ^{9, 20}	\$	Low	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Train staff on individual actions and responsibilities including the Emergency Action Plan, Incident Response Plan, and Unmanned Aircraft System identification and response procedures ^{2, 6}	\$	Low	✓	✓	✓		✓		✓	✓	✓		✓	✓		
Train screening staff on equipment handling, physical searches, and medical screening ^{12, 13, 14}	\$	Low	✓		✓		✓	✓	✓		✓					✓
Conduct exercises on Incident Response Plans of the EAP (Active Shooter, Evacuation, Shelter, Reunification) ^{1, 3, 7, 8, 15}	\$	Low	✓		✓		✓		✓		✓					
Train staff in identifying and responding to suspicious UAS activity ^{2, 21}	\$	Low			✓	✓		✓		✓	✓	✓				
Train staff on procedures for screening special needs visitors and service animals ^{12, 13}	\$	Low	✓		✓		✓		✓							

Security Measure Options

(numbers refer to relevant entries in Resources section)

Threats Mitigated by Security Measure

Cost Level	Complexity Level	Threats Mitigated by Security Measure												Event Cancellation*	Theft/Vandalism*
		Active Shooter	Vehicle Incident	Improvised Explosive Device (IED)	Vehicle-Borne IED (VBIED)	Crowd Control	Chem/Bio WMD	Hostile Patrons	Civil Disturbance	Unmanned Aircraft Systems	Loss of Services/Disruption	Industrial Incident	Natural Disaster/Extreme Weather [Event]		

Perimeter Security

Ensure that venue property boundaries are properly marked and distinguishable to visitors ⁶	\$	Low	✓			✓		✓	✓	✓	✓			✓	
Secure all perimeter entrances that are not staffed ^{6, 8}	\$	Low	✓	✓		✓	✓		✓	✓					✓
Post “No Drone Zone” signs in areas where UAS takeoff or landing is restricted by state or local laws or a flight restriction ^{2, 21}	\$	Low		✓	✓		✓		✓	✓	✓				
Secure ground level access points such as windows ^{6, 8, 18}	\$	Low	✓				✓	✓	✓						✓
Post signs of all prohibited items ^{12, 13}	\$	Low	✓	✓					✓	✓				✓	
Keep shrubbery near gates, entrances, windows, or access points to a minimum ^{6, 18}	\$\$	Mod.	✓	✓				✓	✓					✓	✓
Establish security zones including standoff distances for VBIED ^{6, 22, 23}	\$\$	Mod.		✓	✓	✓						✓		✓	

Access Control

Create public access through dedicated checkpoints only ¹⁴	\$	Low	✓	✓		✓	✓	✓		✓				✓	✓
Ensure designated trained security personnel are present at entry points ¹³	\$	Low	✓			✓	✓	✓	✓	✓				✓	
Conduct a visual search of handbags ^{12, 13}	\$	Low	✓	✓			✓	✓		✓	✓			✓	
Plan restricted areas as necessary and account for access controls, lock management, and credentialing ^{6, 13, 18}	\$	Low	✓	✓							✓				✓
Consider color-coded tickets to assist patrons and staff ^{6, 18}	\$	Low				✓			✓		✓				
Ensure tickets are electronically scanned ¹³	\$	Low	✓			✓									
Establish background checks for all event staff ¹⁸	\$\$	Mod.	✓	✓	✓	✓		✓	✓	✓	✓	✓		✓	✓
Develop an identification system for vehicles allowed into the venue’s inner perimeters ^{23, 24}	\$\$	Mod.		✓		✓	✓		✓	✓			✓		

Security Measure Options

(numbers refer to relevant entries in Resources section)

	Cost Level	Complexity Level	Threats Mitigated by Security Measure											
			Active Shooter	Vehicle Incident	Improvised Explosive Device (IED)	Vehicle-Borne IED (VBIED)	Crowd Control	Chem/Bio WMD	Hostile Patrons	Civil Disturbance	Unmanned Aircraft Systems	Loss of Services/Disruption	Industrial Incident	Natural Disaster/Extreme Weather [Event]
Access Control (cont.)														
Ensure utility areas are alarmed ¹⁰	\$\$	Mod.	✓								✓	✓	✓	
Require photo IDs or other credentials for event staff ^{13, 14}	\$\$	Mod.	✓	✓						✓				✓
Screen all visitors with walk-through metal detectors ^{13, 14}	\$\$\$	High	✓	✓			✓	✓		✓	✓			✓
Crowd Management														
Restrict access to non-public areas ^{4, 6, 8, 18}	\$	Low	✓	✓		✓	✓	✓	✓		✓			✓
Utilize public address systems, social media, email, and message boards to communicate locations, restrictions, evacuation routes and entry control points ¹⁰	\$	Low	✓	✓		✓	✓	✓	✓	✓				✓
Ensure Security and Staff personnel are positioned to assist with end-of-event egress and to monitor for suspicious activity ^{6, 8, 17, 20}	\$	Low	✓	✓		✓		✓	✓					✓
Traffic Management														
Create drop-off areas per the Traffic Management Plan ²³	\$	Low			✓	✓			✓			✓		
Ensure law enforcement officers are present to support traffic flow on public streets ^{17, 19, 23}	\$\$	Low	✓		✓	✓		✓	✓			✓		
Post traffic monitors with safety vests/radio to support traffic flow on venue property ^{17, 23}	\$\$	Mod.	✓		✓	✓		✓	✓			✓		
Emergency Management														
Mark evacuation routes/standoff distance points clearly ^{6, 8, 17}	\$	Low	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	
Test emergency notification systems ¹⁰	\$	Low			✓	✓	✓	✓	✓	✓		✓	✓	
Coordinate with first responders to designate medical triage/EMS staging area in the event of an incident ^{15, 19}	\$\$	Mod.	✓	✓	✓	✓		✓	✓		✓			

GLOSSARY

Access Control: Any combination of barriers, gates, electronic security equipment, and/or guards that ensures only authorized personnel, vehicles, or items are granted entry to a facility or secure area.

Active Shooter: An individual actively engaged in killing or attempting to kill people in a confined and populated area, typically using firearms.

Crowd Control: Utilizing barriers, queue management systems, and staff training for effective crowd control.

Crowd Management: Implementing strategies to ensure safety and orderly behavior of patrons within a venue.

Chemical/Biological Weapon of Mass Destruction (WMD): A chemical weapon of mass destruction is a substance intended to kill, seriously injure, or incapacitate individuals mainly through physiological effects. A biological weapon of mass destruction is a natural or man-made microorganism that causes disease in individuals, plants, animals, or causes matter to deteriorate.

Civil Disturbance: Deliberate and planned acts of violence and destruction stemming from organized demonstrations on or near federal property.

Equipment: Tools or devices used as part of a protective system, including countermeasures such as electronic security system elements and other devices used by personnel to detect and assess threats, weapons, tools, explosives, or chemical, biological, or radiological agents.

Hostile Patron: An individual exhibiting aggressive, violent, or disruptive behavior that poses a threat to a venue.

Improvised Explosive Device (IED): A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract.

Industrial Incident: An unexpected occurrence in an industrial establishment causing bodily injury to at least one person.

Perimeter Security: The implementation of fencing, lighting, and surveillance to secure venue boundaries.

Theft: The unlawful taking, carrying, leading, or riding away of property from the possession or constructive possession of another.

Unmanned Aircraft System (UAS): An unmanned aircraft system is an unmanned aircraft and the equipment necessary for the safe and efficient operation of that aircraft.

Vandalism: The willful or malicious destruction, injury, disfigurement, or defacement of any public or private property, real or personal, without the consent of the owner or person having custody or control. This may include cutting, tearing, breaking, marking, painting, drawing, covering with filth, or any other such means as may be specified by local law.

Vehicle Ramming: Driving a vehicle in an attempt to penetrate a facility (e.g., lobby or loading dock), breach a defined perimeter, or injure/kill individuals.

Vehicle Incident: An unstable situation that includes at least one harmful event (injury or property damage) involving a motor vehicle in transport (in motion, ready for motion, or on a roadway but not parked in a designated parking area) that does not result from a discharge of a firearm or explosive device and does not directly result from a disaster.

Vehicle Borne Improvised Explosive Device (VBIED): A form of explosive attack characterized by using a vehicle as an improvised explosive device.

RESOURCES

1. Active Shooter How to Respond | CISA

A guide to determine the correct actions in the event of an active shooter situation.

cisa.gov/resources-tools/resources/active-shooter-how-respond-booklet

2. Be Air Aware | CISA

CISA's Be Air Aware™ program helps increase awareness of cyber and physical risks posed by unmanned aircraft systems (UAS or drones).

cisa.gov/topics/physical-security/be-air-aware

3. De-Escalation Series | CISA

Four products helping personnel identify and navigate suspicious activity or potentially escalating situations and how to safely disengage and report to the appropriate authorities.

cisa.gov/resources-tools/resources/de-escalation-series

4. Federal Facility Security | CISA

Information on the Interagency Security Committee (ISC), which collaboratively establishes policies, monitors compliance, and enhances the security and protection of Federal Facilities.

cisa.gov/topics/critical-infrastructure-security-and-resilience/federal-facility-security

5. Homeland Threat Assessments | DHS

An annual overview of the most direct and pressing threats to the United States.

dhs.gov/publication/homeland-threat-assessment

6. Mass Gathering Security Planning Tool | CISA

A tool containing a combination of background information, event planning checklist items, and venue characteristics, as well as suggested planning considerations based on the information entered.

cisa.gov/resources-tools/resources/mass-gathering-security-planning-tool

7. Options for Consideration (Active Shooter Preparedness) Video | CISA

A video demonstrating possible actions individuals can take if confronted with an active shooter scenario as well as how to assist authorities once law enforcement arrives.

cisa.gov/resources-tools/resources/options-consideration-video

8. Physical Security Considerations for Temporary Facilities | CISA

A guide detailing the different risk mitigations associated with temporary facilities.

cisa.gov/resources-tools/resources/physical-security-considerations-temporary-facilities-fact-sheet

9. Power of Hello | CISA

Information on procedures that help employees observe and evaluate suspicious behaviors while empowering them to mitigate potential risk and obtain help when necessary.

cisa.gov/topics/physical-security/non-confrontational-techniques/power-hello

10. Priority Telecommunications Services | CISA

CISA offers a suite of technical tools to give calls priority when networks are congested or compromised.

cisa.gov/topics/emergency-communications/priority-services

11. Public Assembly Facilities Recovery Guide | IAVM

A guide assisting all public assembly venues in developing written health and safety guides, education, and training opportunities.

iavm.org/resources/safety-security/

12. Public Venue Bag Search Procedures Guide | CISA

A guide detailing procedures and suggestions for developing and implementing bag searches at public assembly venues hosting a variety of events, such as sporting events, concerts, family festivals, or other public gatherings.

cisa.gov/resources-tools/resources/public-venue-bag-search-procedures-guide

13. Public Venue Security Screening Guide | CISA

A guide providing options for consideration when developing and implementing security screening procedures for major sporting events, concerts, fairs and expos, and similar large gatherings.

cisa.gov/resources-tools/resources/public-venue-security-screening-guide

14. Public Venue Security Screening Guide Touchless Screening Annex | CISA

A guide outlining specific considerations for touchless screening protocols as a supplement to the general screening considerations outlined in the CISA Public Venue Security Screening Guide.

cisa.gov/resources-tools/resources/public-venue-security-screening-guide

15. Attacks in Crowded and Public Spaces | Ready.gov

Information on steps to prepare and protect yourself and help others in the event of an attack.

<https://www.ready.gov/public-spaces>

16. Risk Assessments | Ready.gov

A tool to determine the hazards and risks most likely to cause significant injury and harm.

ready.gov/business/planning/risk-assessment

17. Security Advisors | CISA

Information on CISA's physical and cybersecurity experts who can assist in identifying potential vulnerabilities and strategizing security enhancements.

cisa.gov/about/regions/security-advisors

18. Security Planning Workbook | CISA

A workbook used by individuals involved with an organization's security planning efforts. It will compile key information that can assist in building a comprehensive security plan.

cisa.gov/resources-tools/resources/security-planning-workbook

19. State Fusion Centers | DHS

A resource detailing centers that provide information sharing and analysis services.

dhs.gov/fusion-center-locations-and-contact-information

20. Suspicious Activity and Items | CISA

Information on recognizing unusual behaviors and suspicious items associated with IED threats.

cisa.gov/suspicious-activity-and-items

21. Unauthorized Drone Activity Over Sporting Venues | CISA

This document presents options for sporting venue owners and operators to consider to prevent, protect from, and respond to unauthorized drone activity.

cisa.gov/resources-tools/resources/unauthorized-drone-activity-over-sporting-venues

22. Vehicle Borne IED Identification: Parked Vehicles | CISA

A guide providing key indicators of VBIED attacks.

cisa.gov/resources-tools/resources/vbied-identification-card

23. Vehicle Incident Prevention and Mitigation Guide | CISA

The Vehicle Incident Prevention and Mitigation Security Guide aims to provide vehicle threat mitigation training and recommended options for consideration. It offers an overview of the threat environment and provides resources to help stakeholders strengthen organizational security and safeguard against direct threats and unintentional hazards.

cisa.gov/resources-tools/resources/vehicle-incident-prevention-and-mitigation-security-guide

24. Vehicle Ramming Action Guide | CISA

A guide containing information on indicators, mitigation strategies, and protective measures in the event of a vehicle ramming attack.

cisa.gov/resources-tools/resources/vehicle-ramming-action-guide