



PUBLIC VENUE SECURITY RESOURCES GUIDE

JULY 2026

COMMERCIAL FACILITIES SECTOR

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

CONTENTS

Overview	1
Commercial Facilities Resources	2
Resources to Help Identify and Report Suspicious Behavior	3
Tools, Trainings, and Exercises	5
Tools	5
Trainings.....	5
Cybersecurity Resources and Advisories.....	7
Cybersecurity Resources.....	7
Advisories.....	8
Unmanned Aircraft Systems (UAS) Resources	9
Faith-Based Resources	11
Resources.....	12

LEGEND



Website



Tool



Guide



Video



Factsheet



Assessment



Training



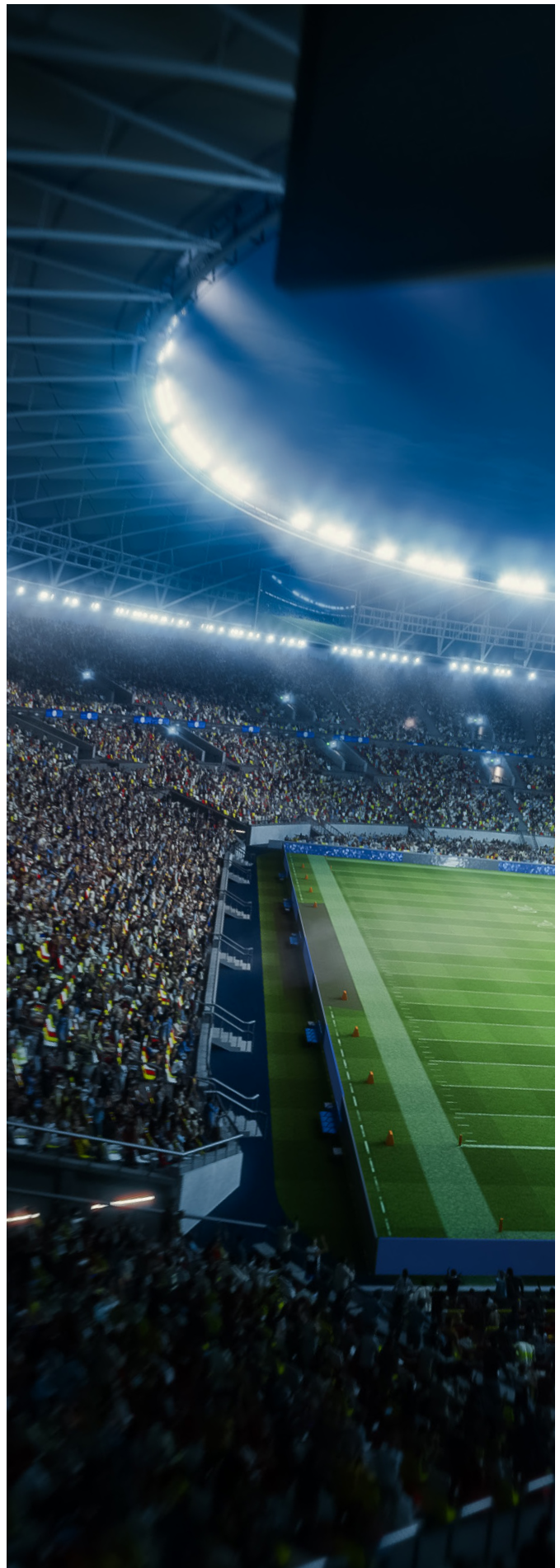
Advisory

OVERVIEW

The Commercial Facilities Sector is comprised of a wide range of sites that attract large crowds for shopping, business, entertainment, and lodging. Many of these facilities operate on the principle of open public access, allowing people to move freely without the hindrance of highly visible security barriers.

The sector is categorized into eight distinct subsectors: 1) Media and Entertainment; 2) Gaming; 3) Lodging; 4) Outdoor Events; 5) Real Estate; 6) Public Assembly; 7) Retail; and 8) Sports Leagues. The Public Assembly Subsector consists of facilities that attract large gatherings of people, such as convention centers, auditoriums, stadiums, arenas, movie theaters, fairgrounds, festivals and parades and cultural properties like museums, zoos, planetariums, aquariums, libraries, and performance venues.

This guide is designed to provide venue managers with resources to strengthen the security and resilience of their facilities against evolving threats. These resources include tools, trainings, and guidance on risk management, cybersecurity considerations, threat awareness, suspicious behavior, and best practices for coordinating with federal state and local partners.



COMMERCIAL FACILITIES RESOURCES

The following resources can assist venue owners and operators with developing a comprehensive incident management and security strategy tailored to their facility's unique needs.



CISA Physical Security

The CISA Physical Security webpage provides resources on a wide variety of threats as well as resources specific to certain public gathering locations (e.g., houses of worship, schools).



CISA Resources and Tools

The search feature on CISA's Resources and Tools webpage can be filtered to show specific Commercial Facilities resources.



Mass Gathering Security Planning Tool

The Mass Gathering Security Planning Tool provides event planners with a framework to begin or continue planning efforts for mass gatherings or special events, and connects stakeholders to the suite of tools and resources provided by CISA and its partners.



Personal Security Considerations Action Guide

The Personal Security Considerations Action Guide provides actionable recommendations and resources to help critical infrastructure workers assess their security posture and prevent and mitigate threats to personal safety.



Hostile Vehicle Mitigation Resources

The Hostile Vehicle Mitigation Resources webpage explores the vehicle ramming mitigation resources offered by CISA and its partners.



Priority Telecommunications Fact Sheet

The Priority Telecommunications Fact Sheet outlines the three priority telecommunications services provided by CISA to enable essential personnel to communicate when networks are degraded or congested due to weather events, mass gatherings, cyberattacks, or events stemming from human error.



Complex Coordinated Attacks Action Guide

The Complex Coordinated Attacks Action Guide provides the critical infrastructure community with information regarding attack vectors used by terrorists and other extremist actors as well as suggested protective measures.



Vehicle Incident Prevention and Mitigation Security Guide

The Vehicle Incident Prevention and Mitigation Security Guide offers a recommended framework of Plan-Prevent-Protect against vehicle threats for critical infrastructure owners and operators, as well as those responsible for pedestrian safety in proximity to those sites.



CISA Active Assailant Security Resources

The CISA Active Assailant Security Resources offers a comprehensive set of courses, materials, and workshops to better prepare organizations to deal with an active assailant situation. These resources focus on behaviors that represent pre-incident indicators and characteristics of active shooters, potential attack methods, how to develop emergency action plans, and the actions that may be taken during an incident.



CISA Security Advisors

CISA Security Advisors provide security and resilience support to critical infrastructure owners and operators, including public venues and spaces. Advisors assist stakeholders through security assessments, risk management support, incident coordination, preparedness resources, and protective security guidance to help organizations strengthen physical and cybersecurity posture against evolving threats.



CISA Securing Public Gatherings

The CISA Securing Public Gatherings webpage provides resources on how CISA fosters collaboration between the private and public sectors to mitigate risk and enhance the security and resilience of public gatherings.

RESOURCES TO HELP IDENTIFY AND REPORT SUSPICIOUS BEHAVIOR

This section includes resources providing employees, citizens, patrons, and others with the skills and support needed to identify and report suspicious behavior.



Are You Ready? Guide

FEMA's Are You Ready? Guide provides general disaster preparedness tips for before, during, and after disasters, as well as best practices to inform preparedness decisions about specific disasters such as hurricanes, earthquakes, and active shooters.



If You See Something, Say Something®

"If You See Something, Say Something®" is a national campaign that raises public awareness of the signs of terrorism and terrorism-related crime as well as how to report suspicious activity to state and local law enforcement.



Insider Threat Mitigation

CISA's Insider Threat Mitigation webpage provides information and resources to help individuals, organizations, and communities create or improve existing insider threat mitigation programs.



Mobilization Indicators Guide

The Mobilization Indicators Guide informs law enforcement, terrorism prevention practitioners, other first responders, community leaders, and the general public about threats of violence and contextual behaviors that suggest an individual is mobilizing to violence.



Office for Bombing Prevention

The Office for Bombing Prevention (OBP) leads the Department of Homeland Security's (DHS) efforts to implement the National Policy for Countering Improvised Explosive Devices and enhance the nation's ability to prevent, protect against, respond to, and mitigate the use of explosives against critical infrastructure, the private sector, and federal, state, local, tribal, and territorial entities.



DHS-DOJ Bomb Threat Guidance Quad-Fold

CISA and the Federal Bureau of Investigation (FBI) developed the DHS-DOJ Bomb Threat Guidance Quad-Fold as a quick reference guide that provides site decision-makers with pre-threat preparation, threat assessment considerations, staff response guidelines, and evacuation and shelter-in-place considerations.



Emergency Action Planning

OSHA Emergency Action Planning is a website to assist with development of an Emergency Action Plan to organize employer and employee actions during workplace emergencies.



Physical Security Considerations for Temporary Facilities

Physical Security Considerations for Temporary Facilities helps temporary facilities – defined as those that are established for set time frames for hosting a venue – navigate their unique security challenges due to their provisional nature.

RESOURCES TO HELP IDENTIFY AND REPORT SUSPICIOUS BEHAVIOR (CONTINUED)



Violence Prevention Through De-escalation

The Violence Prevention Through De-escalation video is designed to help the critical infrastructure community and public gathering locations identify concerning behaviors and mitigate the risk from incidents or targeted violence. The video provides security and non-security professionals with principles and techniques that can augment traditional security protocols.



Employee Vigilance - Power of Hello

The Power of Hello resources provides stakeholders with information to assist in identifying and responding to suspicious behavior. Used effectively, the right words can be a powerful tool when faced with a variety of threats. The Power of Hello approach consists of four steps: Observe, Initiate a Hello, Navigate the Risk, and Obtain Help. To observe, stay vigilant of one's surroundings. Initiating a hello acknowledges a risk which can deter a potential threat. To navigate a risk, one first needs to determine if the behavior you observed is threatening or suspicious. The last step, obtaining help, involves reaching out to management or authorities for assistance in the situation.

TOOLS, TRAININGS, AND EXERCISES

Regular training and exercises are essential for venue managers and staff to effectively respond to security threats and emergencies. There are also tools and workbooks to help commercial facilities owners and operators develop Emergency Action Plans and other security plans for various incidents and situations. This section provides access to tools, tabletop exercises, preparedness drills, cybersecurity training, and emergency response simulations. These tools and resources help ensure staff are well-prepared, improve coordination with law enforcement, and enhance overall venue security.

TOOLS



Active Assailant/Shooter Emergency Action Plan

The Active Assailant/Shooter Emergency Action Plan Product Suite describes the fundamental concepts of developing an Emergency Action Plan (EAP) for an active shooter scenario.



Security Planning Workbook

The Security Planning Workbook is a comprehensive resource that can assist critical infrastructure owners and operators with the development of a foundational security plan. This workbook is designed to be flexible and scalable to suit the needs of most facilities. It is intended for individuals involved with an organization's security planning efforts, including individuals or groups with varying degrees of security expertise, charged with the safety and security of facilities and people.



Vehicle Ramming Self-Assessment

The Vehicle Ramming Self-Assessment Tool was developed in partnership with the Chicago Police Department to assist critical infrastructure owners and operators and federal, state, and local law enforcement agencies with evaluating areas of interest against the risk of a vehicle-ramming style of attack. It is a web-based resource comprised of a series of simple questions that evaluate various components of a facility to assess potential vulnerabilities to a vehicle ramming attack. Based on user responses, the tool provides recommended actions to reduce risk and includes access to a multitude of informational resources.

TRAININGS



Preventing Terrorism

Preventing Terrorism Resources: Training Opportunities offer both in-person and virtual training opportunities with experts on how to prevent violence, respond to emergencies, provide support during mental health crises, and support victims of attacks. Training opportunities are available for the public, educators, law enforcement, health care practitioners, behavioral and mental health professionals, and state, local, tribal, and territorial governments.



Take the Challenge

With the Take the Challenge Homeland Security trainings, learn about paying attention to surroundings.



CISA Incident Management Review [IMR] Training

CISA provides IMR training to help critical infrastructure owners and operators evaluate the processes used to identify and analyze events, declare incidents, determine a response, and improve an organization's incident management capability.

TOOLS, TRAININGS, AND EXERCISES (CONTINUED)

FEMA trainings provide information and guidance on the Incident Command System, the National Incident Management System, and the National Response Framework.



Introduction to the Incident Command System

IS-100.C: Introduction to the Incident Command System (ICS) introduces the ICS and provides the foundation for higher level ICS training. This course describes the history, features, principles, and organizational structure of the ICS. It also explains the relationship between ICS and the National Incident Management System (NIMS).



Basic Incident Command System

IS-200.c: Basic Incident Command System for Initial Response reviews the ICS, provides the context for ICS within initial response, and supports higher level ICS training. This course provides training on, and resources for, personnel who are likely to assume a supervisory position within ICS.



Introduction to the National Incident Management System

IS-700.B: Introduction to the National Incident Management System (NIMS) defines the comprehensive approach guiding the whole community – all levels of government, nongovernmental organizations, and the private sector – to work together seamlessly to prevent, protect against, mitigate, respond to, and recover from the effects of incidents.



National Response Framework, An Introduction

IS-800.D: National Response Framework, An Introduction provides guidance for the whole community. Within this broad audience, this National Response Framework training focuses on those involved in delivering and applying the response core capabilities, including private sector partners, non-governmental organizations (NGOs), government officials, community leaders, emergency management practitioners, and first responders.



National Incident Management System

Emergency Management Institute – National Incident Management System (NIMS) provides training and resources for responders who require advanced application of the ICS by providing overall incident management skills rather than tactical expertise. It emphasizes large scale organizational development, roles and relationships of the command and general staff, and planning, operational, logistical, and fiscal considerations related to large and complex incident and event management.



De-escalation Series for Critical Infrastructure Owners and Operators

The De-escalation Series for Critical Infrastructure Owners and Operators contain four products to assist owners and operators with Recognize, Assess, De-escalate, and Report components.



EXERCISES

CISA Tabletop Exercise Packages

CISA Tabletop Exercise Packages (CTEPs) are a comprehensive set of resources designed to assist stakeholders in conducting their own exercises. Partners can use CTEPs to initiate discussions within their organizations about their ability to address a variety of threat scenarios. With over 100 CTEPs available, stakeholders can easily find resources to meet their specific exercise needs.

CYBERSECURITY RESOURCES AND ADVISORIES

There are a variety of foundational cybersecurity resources for venue managers. This section includes risk management frameworks, emergency preparedness guidelines, and best practices. These resources help venue operators identify vulnerabilities, enhance safety measures, and coordinate with public and private security partners to strengthen overall resilience. CISA and other federal agencies also issue cybersecurity advisories, highlighting specific incidents, vulnerabilities, and threats for critical infrastructure sectors.

CYBERSECURITY RESOURCES



Cybersecurity Evaluation Tool (CSET)®

The Cybersecurity Evaluation Tool (CSET)® is a no-cost stand-alone desktop application that systematically guides critical infrastructure owners and operators through evaluating their operational and informational technology.



CISA Industrial Control Systems (ICS) Training

CISA offers no-cost ICS training to help protect critical infrastructure against cyberattacks. ICS training is provided in two formats: web-based training and instructor-led training.



Cross-Sector Cybersecurity Performance Goals

The Cross-Sector Cybersecurity Performance Goals are a subset of cybersecurity practices, selected through a thorough process of industry, government, and expert consultation, aimed at meaningfully reducing risks to both critical infrastructure operations and the American people.



Cyber Incident Reporting for Critical Infrastructure Act

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCA) requires CISA to develop and implement regulations that require covered entities to report covered cyber incidents and ransomware payments to CISA. These reports allow CISA to rapidly deploy resources and render assistance to victims suffering attacks, analyze incoming reporting across sectors to spot trends, and quickly share that information with network defenders to warn other potential victims.



Defending OT Operations Against Ongoing Pro-Russia Hacktivist

The Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity Fact Sheet provides information and mitigations associated with cyber operations conducted by pro-Russia hacktivists who seek to compromise ICS and small-scale operational technology systems in North American and European critical infrastructure sectors.



Cybersecurity Tools

As part of a continuing mission to reduce cybersecurity risk across U.S. critical infrastructure partners and state, local, tribal, and territorial governments, CISA compiled a list of no-cost cybersecurity tools and services to help organizations further advance their security capabilities. This living repository includes cybersecurity services provided by CISA, widely used open-source tools, and no-cost tools and services offered by private and public sector organizations across the cybersecurity community.



High-Risk Communities

High-Risk Communities can use these upskilling modules and resource links, which focus on cybersecurity for high-risk communities. These communities are a uniquely attractive target for cyber threat actors due to their lean budgets and potential inability to significantly invest in cybersecurity. Threat actors leverage cyber intrusions to undermine the fundamental values and interests common to free societies.

CYBERSECURITY RESOURCES AND ADVISORIES

(CONTINUED)



[Stop Ransomware](#)

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Stop Ransomware is the U.S. government's official one-stop location for resources to tackle ransomware more effectively.



ADVISORIES

[Scattered Spider](#)

CISA and the FBI released the Cybersecurity Advisory (CSA) on Scattered Spider in response to activity by Scattered Spider threat actors against the Commercial Facilities Sector and Subsectors. This advisory provides tactics, techniques, and procedures (TTPs) obtained through FBI investigations.



[#StopRansomware: ALPHV Blackcat](#)

With the increase in related activity affecting the Healthcare and Public Health Sector, the updated #StopRansomware: ALPHV Blackcat advisory, now joint sealed with the Department of Health and Human Services (HHS), contains new indicators of compromise and TTPs associated with the ALPHV Blackcat ransomware.



[#StopRansomware: Black Basta](#)

The joint #StopRansomware: Black Basta CSA reports on a ransomware variant whose actors have encrypted and stolen data from at least 12 out of 16 critical infrastructure sectors, including the Healthcare and Public Health Sector.



[CISA Cybersecurity Alerts and Advisories](#)

CISA regularly updates its Cybersecurity Alerts and Advisories webpage, providing venue owners and operators with the most up-to-date cybersecurity threats and mitigation measures.

UNMANNED AIRCRAFT SYSTEMS (UAS) RESOURCES

Public venues face increased risk from UAS, also known as drones, flying over venues during events and on non-event days. Additionally, venues may use UAS as part of their security program. This section provides guidance to venue owners and operators on ensuring patron and staff safety should a UAS intrusion happen during an event.

It also highlights security considerations venue teams should take when developing a UAS plan for their own use.



Be Air Aware™

CISA's Be Air Aware™ program helps increase awareness of cyber and physical risks posed by UAS. The resources on the Be Air Aware™ webpage provide essential, ready-to-use information about UAS threats and steps to effectively manage risk to critical infrastructure and public gatherings.



Cybersecurity Guidance: Chinese-Manufactured UAS

CISA and the FBI released the Cybersecurity Guidance: Chinese-Manufactured UAS to raise awareness on the threats posed by Chinese-manufactured UAS and provide UAS cybersecurity recommendations to reduce risks to networks and sensitive information.



Secure Your Drone: Privacy and Data Protection Guidance

Secure Your Drone: Privacy and Data Protection Guidance provides guidance for drone users to protect their data and privacy before, during, and after flying their drone. It also provides additional resources to augment an organization's preparedness, response, and resilience. Any venue staff member working with drones as part of a venue's security plan should be familiar with the guidance provided in this resource to ensure the safety and security of the venue and its systems.



Unauthorized Drone Activity Over Sporting Venues

The Unauthorized Drone Activity Over Sporting Venues product provides options for sporting venue owners and operators to consider to prevent, protect from, and respond to unauthorized drone activity over their venues, which pose a risk to patrons and staff. This product provides tangible actions that owners and operators can take to improve an organization's capabilities to secure its people, systems, and facilities from unauthorized drone activity.



Suspicious Unmanned Aircraft System Activity Guidance

This guidance provides venue owners and operators with considerations for identifying, documenting, and reporting suspicious UAS activity occurring near facilities, events, and public gatherings. The resource supports security planning and incident response efforts by outlining key reporting considerations and coordination pathways to help improve situational awareness and security posture related to unauthorized UAS activity.



Safe Handling Considerations for Downed Unmanned Aircraft Systems

This guidance provides safety and security considerations for personnel who encounter downed, crashed, or abandoned UAS. This resource outlines potential hazards associated with damaged UAS platforms, including battery fires, hazardous materials, suspicious payloads, and evidentiary concerns, while providing recommended actions to support safe response, reporting, and coordination with appropriate authorities.

UNMANNED AIRCRAFT SYSTEMS (UAS) RESOURCES (CONTINUED)



Unmanned Aircraft System Detection Technology Guidance

This guidance provides an overview of UAS detection technologies and operational considerations that organizations should evaluate when assessing potential UAS detection capabilities. The resource helps stakeholders better understand detection limitations, planning considerations, and factors impacting operational effectiveness to support informed security planning decisions.



Temporary Flight Restrictions

Temporary flight restrictions can be an important security measure to consider for certain large public gathering events. While flight restrictions are in place for many major sporting events via the Sporting Event Notice to Airmen (NOTAM 0/0367), event organizers and federal, state, local, tribal, and territorial law enforcement may also be able to request UAS temporary flight restrictions for other high risk special events using 49 U.S. C. § 44812 or 14 CFR 99.7 process.



Suspicious UAS Identification Poster and Postcard

Provides visual awareness materials designed to help stakeholders recognize suspicious activity, understand potential indicators of concern, and support timely reporting to appropriate authorities.

FAITH-BASED RESOURCES

Houses of worship and faith-based venues face unique security challenges. This section provides guidance on risk management, emergency preparedness, and threat mitigation tailored to faith-based organizations. Resources include security best practices, cybersecurity protections, and training opportunities to help safeguard congregations while maintaining an open and welcoming environment.



Protecting Houses of Worship Resources

The Protecting Houses of Worship Resources webpage is designed to guide users through a four-step process that can act as the building blocks for improving the security and safety of an organization's congregants and facilities.



Six Steps to Enhance Security Against Targeted Violence

CISA, in partnership with the FBI, developed the Protecting Places of Worship: Six Steps to Enhance Security Against Targeted Violence Fact Sheet to outline actions that faith-based organizations and community leaders can take to increase security, focusing on six overarching steps. This product details how taking these six steps can help protect places of worship against potential threats of targeted violence in a cost-effective manner while maintaining an open and welcoming environment.

RESOURCES

Commercial Facilities Resources

Cybersecurity and Infrastructure Security Agency. (N.D.). Physical Security. Retrieved December 5, 2025. Available from <https://www.cisa.gov/topics/physical-security>.

Cybersecurity and Infrastructure Security Agency. (N.D.). All Resources and Tools. Retrieved December 5, 2025. Available from https://www.cisa.gov/resources-tools/all-resources-tools?f%5B0%5D=multiple_resource_sector%3A9&page=0.

Cybersecurity and Infrastructure Security Agency. (N.D.). Securing Public Gathering. Retrieved December 5, 2025. Available from <https://www.cisa.gov/topics/physical-security/securing-public-gatherings>.

Cybersecurity and Infrastructure Security Agency. (2024). Mass Gathering Security Planning Tool. Retrieved December 5, 2025. Available from <https://www.cisa.gov/resources-tools/resources/mass-gathering-security-planning-tool>.

Cybersecurity and Infrastructure Security Agency. (2024). Personal Security Consideration Action Guide. Retrieved December 5, 2025. Available from <https://www.cisa.gov/resources-tools/resources/personal-security-considerations-action-guide>.

Cybersecurity and Infrastructure Security Agency. (N.D.). Hostile Vehicle Mitigation Resources. Retrieved December 5, 2025. Available from <https://www.cisa.gov/topics/physical-security/vehicle-ramming-mitigation/resources>.

Cybersecurity and Infrastructure Security Agency. (2024). Vehicle Incident Prevention and Mitigation Security Guide. Retrieved December 5, 2025. Available from <https://www.cisa.gov/resources-tools/resources/vehicle-incident-prevention-and-mitigation-security-guide>.

Cybersecurity and Infrastructure Security Agency. (2025). Priority Telecommunications Services (PTS). Retrieved December 5, 2025. Available from https://www.cisa.gov/sites/default/files/2025-03/Priority%20Telecommunications%20Services_Overview-2-26-25508Compliant.pdf.

Cybersecurity and Infrastructure Security Agency. (N.D.). Active Assailant Security Resources. Retrieved December 5, 2025. Available from <https://www.cisa.gov/topics/physical-security/active-shooter-preparedness/active-assailant-security-resources>.

Cybersecurity and Infrastructure Security Agency. (2022) Complex Coordinated Attacks: Security Awareness for Soft Targets and Crowded Places. Retrieved December 5, 2025. Available from <https://www.cisa.gov/sites/default/files/2022-11/Action%20Guide%20CCA%20508%20FINAL%2020190905.pdf>.

Cybersecurity and Infrastructure Security Agency. (N.D.) Security Advisors. Retrieved May 29, 2026. Available from <https://www.cisa.gov/about/regions/security-advisors>.

Resources to Help Identify and Report Suspicious Behavior

Federal Emergency Management Agency. (2022) Are You Ready? Guide. Retrieved December 5, 2025. Available from <https://www.ready.gov/collection/are-you-ready>.

Department of Homeland Security. (N.D.) If You See Something, Say Something. Retrieved December 5, 2025. Available from <https://www.dhs.gov/see-something-say-something>.

Cybersecurity and Infrastructure Security Agency. (N.D.). Insider Threat Mitigation. Retrieved December 5, 2025. Available from <https://www.cisa.gov/topics/physical-security/insider-threat-mitigation>.

Office of the Director of National Intelligence. (2021). US Violent Extremist Mobilization Indicators. Retrieved December 5, 2025. Available from https://www.dni.gov/files/NCTC/documents/news_documents/Mobilization_Indicators_Booklet_2021.pdf.

Cybersecurity and Infrastructure Security Agency. (N.D.). Homeland Security - Office for Bombing Prevention (OBP). Retrieved December 5, 2025. Available from <https://www.cisa.gov/topics/physical-security/bombing-prevention>.

Cybersecurity and Infrastructure Security Agency. (2025). DHS-DOJ Bomb Threat Guidance Quad-Fold. Retrieved December 5, 2025. Available from <https://www.cisa.gov/resources-tools/resources/dhs-doj-bomb-threat-guidance-quad-fold>.

Occupational Safety and Health Administration. (N.D.) Evacuation Plans and Procedures: Emergency Action Plan. Retrieved December 5, 2025. Available from <https://www.osha.gov/etools/evacuation-plans-procedures/eap>.

Cybersecurity and Infrastructure Security Agency. (2022) Physical Security Considerations for Temporary Facilities Fact Sheet. Retrieved December 5, 2025. Available from <https://www.cisa.gov/resources-tools/resources/physical-security-considerations-temporary-facilities-fact-sheet>.

Cybersecurity and Infrastructure Security Agency. (2024). Violence Prevention through De-escalation Video. Retrieved December 5, 2025. Available from <https://www.cisa.gov/resources-tools/resources/violence-prevention-through-de-escalation-video>.

Cybersecurity and Infrastructure Security Agency. (N.D.). Employee Vigilance – Power of Hello. Retrieved December 8, 2025. Available from <https://www.cisa.gov/topics/physical-security/conflict-prevention/power-hello>.

Tools, Trainings, and Exercises

- Cybersecurity and Infrastructure Security Agency.** (N.D.). Active Assailant/Shooter Emergency Action Plan Product Suite. Retrieved December 8, 2025. Available from <https://www.cisa.gov/resources-tools/resources/active-shooter-emergency-action-plan-product-suite>.
- Cybersecurity and Infrastructure Security Agency.** (2023). Security Planning Workbook. Retrieved December 8, 2025. Available from <https://www.cisa.gov/resources-tools/resources/security-planning-workbook>.
- Department of Homeland Security.** (N.D.). Prevention Resource Finder: Training Opportunities. Retrieved December 8, 2025. Available from <https://www.dhs.gov/prevention/clearinghouse-category/training-opportunities>.
- Department of Homeland Security.** (N.D.). Take the Challenge. Retrieved December 8, 2025. Available from <https://www.dhs.gov/see-something-say-something/take-challenge>.
- Cybersecurity and Infrastructure Security Agency.** (N.D.). Incident Management Review (IMR) Training. Retrieved December 8, 2025. Available from <https://www.cisa.gov/resources-tools/training/incident-management-review-imr-training>.
- Federal Emergency Management Agency.** (2018). IS-100.C: Introduction to the Incident Command System, ICS 100. Retrieved December 8, 2025. Available from <https://training.fema.gov/is/courseoverview.aspx?code=IS-100.c&lang=en>.
- Federal Emergency Management Agency.** (2019). IS-200.C: Basic Incident Command System for Initial Response, ICS-200. Retrieved December 8, 2025. Available from <https://training.fema.gov/is/courseoverview.aspx?code=IS-200.c&lang=en>.
- Federal Emergency Management Agency.** (2018). IS-700.B: An Introduction to the National Incident Management System. Retrieved December 8, 2025. Available from <https://training.fema.gov/is/courseoverview.aspx?code=IS-700.b&lang=en>.
- Federal Emergency Management Agency.** (2020). IS-800.D: National Response Framework, An Introduction. Retrieved December 8, 2025. Available from <https://www.fema.gov/emergency-managers/national-preparedness/frameworks/response>.
- Federal Emergency Management Agency.** (N.D.). National Incident Management System (NIMS). Retrieved December 8, 2025. Available from <https://training.fema.gov/nims/>.
- Cybersecurity and Infrastructure Security Agency.** (2021). De-escalation Series. Retrieved December 8, 2025. Available from <https://www.cisa.gov/resources-tools/resources/de-escalation-series>.
- Cybersecurity and Infrastructure Security Agency.** (2021). CISA Tabletop Exercises Packages. Retrieved December 8, 2025. Available from <https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages>.

Cybersecurity Resources and Advisories

- Cybersecurity and Infrastructure Security Agency.** (2024). Cyber Security Evaluation Tool (CSET) Fact Sheet for Public Safety. Retrieved December 8, 2025. Available from <https://www.cisa.gov/resources-tools/resources/cyber-security-evaluation-tool-cset-fact-sheet-public-safety>.
- Cybersecurity and Infrastructure Security Agency.** (N.D.). ICS Training Available Through CISA. Retrieved December 8, 2025. Available from <https://www.cisa.gov/resources-tools/programs/ics-training-available-through-cisa>.
- Cybersecurity and Infrastructure Security Agency.** (N.D.). Cross-Sector Cybersecurity Performance Goals. Retrieved December 8, 2025. Available from <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>.
- Cybersecurity and Infrastructure Security Agency.** (2022). Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCA). Retrieved December 8, 2025. Available from <https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia>.
- Cybersecurity and Infrastructure Security Agency.** (2024). Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity. Retrieved December 8, 2025. Available from <https://www.cisa.gov/resources-tools/resources/defending-ot-operations-against-ongoing-pro-russia-hacktivist-activity>.
- Cybersecurity and Infrastructure Security Agency.** (N.D.). No-Cost Cybersecurity Services and Tools. Retrieved December 8, 2025. Available from <https://www.cisa.gov/resources-tools/resources/no-cost-cybersecurity-services-and-tools>.
- Cybersecurity and Infrastructure Security Agency.** (N.D.). High-Risk Communities. Retrieved December 8, 2025. Available from <https://www.cisa.gov/audiences/high-risk-communities>.
- Cybersecurity and Infrastructure Security Agency.** (N.D.). Stop Ransomware. Retrieved December 8, 2025. Available from <https://www.cisa.gov/stopransomware>.
- Cybersecurity and Infrastructure Security Agency.** (2025). Scattered Spider. Retrieved December 8, 2025. Available from <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a>.

Cybersecurity and Infrastructure Security Agency. (2024). #StopRansomware: ALPHV Blackcat. Retrieved December 8, 2025. Available from <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a>.

Cybersecurity and Infrastructure Security Agency. (2024). #StopRansomware: Black Basta. Retrieved December 8, 2025. Available from https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a?utm_source=EA&utm_medium=stakeholder_note&utm_campaign=SRW.

Cybersecurity and Infrastructure Security Agency. (N.D.) Cybersecurity Alerts & Advisories. Retrieved December 8, 2025. Available from <https://www.cisa.gov/news-events/cybersecurity-advisories>.

Unmanned Aircraft Systems (UAS) Resources

Cybersecurity and Infrastructure Security Agency. (N.D.). Be Air Aware. Retrieved December 8, 2025. Available from <https://www.cisa.gov/topics/physical-security/be-air-aware>.

Cybersecurity and Infrastructure Security Agency. (2024). Cybersecurity Guidance: Chinese-Manufactured UAS. Retrieved December 8, 2025. Available from <https://www.cisa.gov/topics/physical-security/be-air-aware/uas-cybersecurity>.

Cybersecurity and Infrastructure Security Agency. (N.D.). Secure Your Drone: Privacy and Data Protection Guidance. Retrieved December 8, 2025. Available from <https://www.cisa.gov/topics/physical-security/be-air-aware/uas-cybersecurity>.

Cybersecurity and Infrastructure Security Agency. (2024). Unauthorized Drone Activity Over Sporting Venues. Retrieved December 8, 2025. Available from <https://www.cisa.gov/topics/physical-security/be-air-aware/protect-critical-infrastructure-and-public-gatherings>.

Cybersecurity and Infrastructure Security Agency. (2025). Suspicious Unmanned Aircraft System Activity Guidance. Retrieved May 29, 2026. Available from <https://www.cisa.gov/resources-tools/resources/suspicious-unmanned-aircraft-system-activity-guidance>.

Cybersecurity and Infrastructure Security Agency. (2025). Safe Handling Considerations for Downed Unmanned Aircraft Systems. Retrieved May 29, 2026. Available from <https://www.cisa.gov/resources-tools/resources/safe-handling-considerations-downed-unmanned-aircraft-systems>.

Cybersecurity and Infrastructure Security Agency. (2025). Unmanned Aircraft System Detection Technology Guidance. Retrieved May 29, 2026. Available from <https://www.cisa.gov/resources-tools/resources/unmanned-aircraft-system-detection-technology-guidance>.

Federal Aviation Administration. (2026). Chapter 20. Temporary Flight Restrictions (TFRs). Retrieved May 29, 2026. Available from https://www.faa.gov/air_traffic/publications/atpubs/foa_html/chap20_section_1.html.

Cybersecurity and Infrastructure Security Agency. (2025). Suspicious UAS Identification Poster and Postcard. Retrieved May 29, 2026. Available from <https://www.cisa.gov/resources-tools/resources/suspicious-uas-identification-poster-and-postcard>.

Faith-Based Resources

Cybersecurity and Infrastructure Security Agency. (N.D.). Protecting Houses of Worship Resources. Retrieved December 8, 2025. Available from <https://www.cisa.gov/topics/physical-security/protecting-houses-worship/resources>.

Cybersecurity and Infrastructure Security Agency. (2023). Protecting Places of Worship: Six Steps to Enhance Security Against Targeted Violence Fact Sheet. Retrieved December 8, 2025. Available from <https://www.cisa.gov/resources-tools/resources/protecting-places-worship-six-steps-enhance-security-against-targeted-violence-fact-sheet>.