Today’s Agenda

A guide to today’s discussion
Our Work

The Cybersecurity and Infrastructure Security Agency (CISA) works with partners to defend against today’s threats and collaborating to build more secure and resilient infrastructure for the future.

Goal 1 - Defend Today
Goal 2 - Secure Tomorrow
School Safety

Given the evolving threat landscape, we must continue to work together to safeguard the Nation and be vigilant in our efforts to identify and prevent incidents of terrorism and targeted violence within the broader community.
CISA’s School Safety Perspective

Capacity builder and integrator for school safety across the federal government

Build safety and resiliency for the Nation’s schools and academic institutions

Our Priorities & Actions:

• **Build capacity** for schools and communities to prevent violence and mitigate impacts of instances of violence;
• **Educate school communities** on the resources available, how to utilize them effectively, and how to prioritize resources based on unique needs;
• Lead the **Federal School Safety Clearinghouse** to coordinate Federal efforts to make schools secure and resilient; and
• Provide **one-stop access through SchoolSafety.gov** to school safety resources and programs.
Building a Network of Safety Partners

**WEBINAR SERIES**

**CONFERENCE & ENGAGEMENTS**

**DIRECT OUTREACH**

**GOV DELIVERY BULLETINS**

**SOCIAL MEDIA**

**STATE PARTNER NETWORK**
- State Departments of Education
- School Safety Centers
- Superintendent Associations
- School Districts & Administrators

**FEDERAL PARTNER NETWORK**
- Department of Education
- Department of Homeland Security
- Department of Justice
- Department of Health & Human Services

**PRIVATE SECTOR NETWORK**
- Educational Organizations & Associations
- School Safety Organizations
- Communities with School Violence Experience
- School Safety Conferences

**ENHANCE SECURITY & PROTECT SCHOOLS’ EDUCATIONAL MISSION**
Risks and Emerging Environments

Establishing a multidisciplinary threat assessment team of school personnel including faculty, staff, administrators, coaches, and available school resource officers who will direct, manage, and document the threat assessment process.
Instances of School Violence

The list of school violence incidents is not intended to be exhaustive, but rather to illustrate the breadth of the problem.

Source: Federal Commission on School Safety
Key Statistics on Risk Environment

- **91%** of school attackers had observable psychological (depression, suicidal ideation, anger, psychotic symptoms, etc.), behavioral (defiance, poor impulse control, violation of social norms, etc.), or neurological (developmental delays, cognitive deficits, etc.) symptoms.

- **80%** of school attackers were bullied by their classmates. Some of the attackers actively sought help to address bullying but received an ineffective response or no response at all.

- **51%** of school attackers had engaged in observable planning behaviors prior to the attack.

- **94%** of school attackers had experienced a risk factor within six months of their attack.

Source: U.S. Secret Service National Threat Assessment Center
In the coming months, **DHS expects the threat environment to become more dynamic** as several high-profile events could be exploited to justify acts of violence against a range of possible targets:

- **Targets could include** public gatherings, faith-based institutions, schools, racial and religious minorities, government facilities and personnel, U.S. critical infrastructure, the media, and perceived ideological opponents.

- **Threat actors** have recently **mobilized to violence** due to factors such as personal grievances, reactions to current events, and adherence to violent extremist ideologies, including racially or ethnically motivated or anti-government/antiauthority violent extremism.

[dhs.gov/national-terrorism-advisory-system](dhs.gov/national-terrorism-advisory-system)
Prevalent Risk Environment Trends

Cybersecurity
1,331 publicly disclosed school cyber incidents affecting U.S. school districts since 2016

Targeted Violence
76% of attackers acquired their firearm from the home of a parent or another close relative

Bombing
2,566 bombing-related incidents at K-12 schools from 2017 to 2022

Mental Health
30% of students reported feeling unhappy and depressed more than usual since the pandemic

Sources: K12 SIX, TRIPwire’s OSINT IED Database, U.S. Secret Service National Threat Assessment Center, America’s Promise Alliance
Planning for and implementing a school physical security system is a complex undertaking, and local education agencies will need to navigate myriad challenges as they engage in the process. The 3rd Edition of the K-13 School Security Guide address Common Challenges and Tradeoffs to help schools identify how measures may affect and interact with efforts to prevent violence.

Common Challenges At-A-Glance:

- Policies (Federal, State, Local)
- Seeking Approval (Administration, Board)
- Funding (Initial, Long Term)
- Use and Effectiveness of Measures
- Understanding Limitations (Physical, CRCL, Technology)
The knowledge of how to plan is critical in emergency of a disaster, including saving lives and protecting property, and helping a community recover more quickly from a disaster.
Cycle of Preparedness

**Recognition**
- Form Planning Team
  - Incident Analysis
  - Mission Areas
  - Planning Principles
  - Planning Team

**Prevention**
- Conduct Risk Assessment
  - Pathway to Violence
  - Report Behavior
  - Work Place Violence
  - Risk Issues

**Protection**
- Establish Goals and Objectives
  - Site Vulnerabilities
  - Physical Security
  - Internal Factors
  - Goals and Objectives

**Mitigation**
- Assess Courses of Action
  - Reduce Impact
  - Communications
  - Develop Courses of Action
  - Format Plan

**Response**
- Draft Plan and Approve
  - Steps to Save Lives
  - Response Coordination
  - Disability Planning
  - Approve the plan

**Recovery**
- Training and Exercise
  - Short-Term Recovery
  - Long-Term Recovery
  - Continuity of Operations/Continuity of Government
  - Training and Exercises

- Team Identified
- Risks Identified
- Goals/Objectives Defined
- Courses of Action Identified
- Plan Outlined
- Plan Implemented
The planning process involves working collaboratively with a team to understand and determine EOP goals and objectives. The planning process is flexible and should be adapted to the IHE’s unique characteristics and the situation.

**The Planning Process**

**STEP 1:** Form Planning Team
- Identify Core Planning Team
- Form a Common Framework
- Define and Assign Roles
- Determine a Meeting Schedule

**STEP 2:** Conduct Risk Assessment
- Identify Threats and Hazards
- Assess Risk
- Prioritize Risk and Hazards

**STEP 3:** Establish Goals and Objectives
- Develop Goals
- Develop Objectives

**STEP 4:** Assess Courses of Action
- Identify Courses of Action
- Identify Resources
- Assign COAs to Positions

**STEP 5:** Draft Plan & Approve
- Format the Plan
- Write the Plan
- Review the Plan
- Approve and Share the Plan

**STEP 6:** Training and Exercise
- Train Stakeholders
- Exercise the Plan
- Review, Revise and Maintain the Plan

[cisa.gov/active-shooter-preparedness](https://cisa.gov/active-shooter-preparedness)
Developing a Security Plan

- **Each school / facility is unique**
  Tailor your security plan to meet the needs of your school / district

- **Apply systems-based approach to layered security**
  An integrated approach of multiple security resources helps mitigate single points of failure

- **Building a team & culture**
  A multi-disciplinary team will serve to create a more representative security plan and to ensure that the needs of diverse stakeholders are met

[cisa.gov/k-12-school-security-guide](cisa.gov/k-12-school-security-guide)
Planning: The Systems-Based Approach

Taking a systems-based approach to school physical security means ensuring that various security measures across a school campus work together in an integrated way, and that planning also incorporates the relevant policies and training programs that must also be in place for the entire system to function effectively.

The Systems-Based Approach At-A-Glance:

- Understand the five core elements of school physical security
- Consider a school’s specific circumstances to tailor measures
- Identify the various security layers that exist at the school
- Determine security efforts in alignment with P-PM-RR
- Engage in the school security physical planning process
The security annex should focus on: How agreements with law enforcement agencies address the daily role of law enforcement officers in and around campus

- How to help ensure the buildings and facilities are physically secure
- How to assist students, faculty, and staff in safely traveling to, from, and within the campus framework
- How to respond to threats identified by the Threat assessment Team
- How to address issues related to cybersecurity and threats to information technology systems
- How security will be provided at stadiums, arenas, and other large-event facilities
- How to provide security for sensitive facilities, including research labs and test reactors on the campus
- How to account for students, faculty, staff, and visitors in a variety of locations at different points in the day
- How information will be shared with law enforcement officers or other responders
Planning: Connect, Plan, Train, and Report

CISA encourages applying **four steps** in advance of an incident or attack that can help better prepare us to proactively think about our roles in safety and security of our schools and communities.

- **CONNECT:** Reach out and develop relationships in your community, including local law enforcement. Having these relationships established before an incident occurs can help speed up the response when something happens.

- **PLAN:** Take the time now to plan on how you will handle a security event should one occur. Learn from other events to inform your plans.

- **TRAIN:** Provide your employees with training resources and exercise your plans often. The best laid plans must be exercised in order to be effective.

- **REPORT:** “If You See Something, Say Something™” is more than just a slogan. Call local law enforcement.

For more information on insider threat mitigation, please send an email to InTmitigation@cisadhs.gov
## Election Security Planning

**School facilities** often serve as polling places. While we try to maintain the sanctity of the election process, the safety of students, faculty and staff remain the primary responsibility. The following are several ideas and suggestions to keep in mind as schools prepare for Election Day.

### Prior to Election
- Ensure parents/guardians, students, and staff are properly notified
- Review protocols: bomb threats, protests, lockdown, and evacuation with staff.
- Check communication and announcement systems
- Consider increasing security measures
- Consider distance learning on Election Day
- Coordinate the delivery and set-up of the election equipment with the clerk’s office.
- Separate the voting areas from offices and classrooms
- Work with election staff to provide guidance on emergency actions and responses for election staff
- Make election staff aware of the site’s camera system so voting booths can be positioned accordingly. Do not remove cameras on Election Day

### During the Election
- Establishing pre-determined modes of communication with the election staff stationed at your facilities.
- Share your emergency/evacuations routes and shelter locations and share any changes to your daily routine with students and families.
- Assign teams to check the campus grounds before the start of classes on the morning of the election, watching for anything suspicious.
- Coordinate with volunteers to assist the campus in monitoring voter interaction with students.
- Remind faculty and staff to wear and display their official district identification
- Continue open communication and set limits with election staff assigned to your building

### After the Election
- Assign a team to check the campus grounds before the start of classes the day after the election, watching for anything suspicious.
- Thoroughly clean and disinfect voting areas to stop the spread of COVID-19, along with other seasonal viruses.
- Work with election officials to ensure the prompt removal of election equipment from school property.

---

*Be Vigilant!*
Our Resources

CISA resources provides users with access to information on services across all CISA’s mission areas that are available to Federal Government; State, Local, Tribal and Territorial Government; Private Industry; Academia; and NGO and Non-Profit stakeholders.
Violence Prevention

Given the evolving threat landscape, we must continue to work together to safeguard the Nation and be vigilant in our efforts to identify and prevent incidents of terrorism and targeted violence within the broader community.
CTIC is the designated fusion center for the State of Connecticut and is one of 80 fusion centers in the country. Fusion centers increase collaboration and information sharing between all levels of government. Fusion centers serve as the focal point for the receipt, analysis, and sharing of threat-related information between State, Local, Tribal and Territorial (SLTT), federal, and private sector entities.

- **Counter Terrorism and Intelligence**: incorporates a variety of methods to prevent or thwart a terrorist attack. In Connecticut, DEMHS and the CT State Police share responsibilities for counter terrorism in the state.

- **Critical Infrastructure Protection**: The Connecticut Critical Infrastructure Protection Unit (CIPU) works to assess and protect Connecticut’s public and private critical infrastructure assets and key resources, both physical and cyber-based, that are essential to maintaining the minimal operational capabilities of government and are necessary to the well-being of the economy.

- **Cybersecurity**: the Connecticut Intelligence Center (CTIC) works to protect entities in the State of Connecticut from cyber-attacks by providing tactical intelligence that can be used to detect malicious behavior and by providing strategic intelligence aimed at reducing potential vulnerability.

To get on the Fusion Center Email Listing Contact: ctic@ct.gov
The Office of Emergency Management provides a coordinated, integrated program for state-wide emergency management and homeland security, including coordination of the state response to emergencies, strategic and operational all-hazards planning; community preparedness; exercise and training; and grants planning and program management.

Averting Targeted School Violence
Helping Children Cope with a Gun Violence Tragedy - English
Helping Children Cope with a Gun Violence Tragedy - Spanish
How to Talk to Young People in the Aftermath of Shootings
Protecting America's Schools
School Security Frequently Asked Questions

DEMHS Regions
Community Preparedness
Planning for All Hazards
Disaster Recovery
Interoperable & Emergency Communication
Radiological Emergency Preparedness
Training and Exercise
School Safety and Security
Citizen Corps
Child Emergency Preparedness
Urban Search and Rescue
Resources: Hometown Security

- CISA’s Hometown Security program provides access to tools and resources to support community security and resilience.

- DHS recognizes that communities are the first line of defense in keeping the public safe and secure.

- **Bomb-Making Materials Awareness Program (BMAP)**
- **Vehicle Ramming Self-Assessment tool**
- **Autonomous Ground Vehicle Security Guide**
- **Sector Spotlight: Cyber-Physical Security Considerations for the Electricity Sub-Sector**
- **Stadium Spotlight: Connected Devices and Integrated Security Considerations**
- **Cybersecurity and Physical Security Convergence Guide**
- **Homeland Threat Assessment**
- **Personal Security Considerations**
- **Protecting Infrastructure During Public Demonstrations**
- **Outdoor Eating Venue Fact Sheet**
- **Suspicious or Unattended poster**
- **Bomb Threat Guidance**
- **Vehicle-Borne IED Identification**
A starting place for DHS documents, resources and tools related to school safety and security.

School Safety and Security | CISA

- K-12 School Security Guide and Companion Products
- SchoolSafety.gov
- National School Safety Summit
- Enhancing School Safety Using a Threat Assessment Model
- Active Shooter Preparedness: School Security and Resilience
- School Safety SIMEX After Action Report
- Key Considerations
- Creating a Targeted Violence Prevention Plan
- Download School Safety and Security Guides
- Campus Resilience Program Resource Library
- Additional Information
SchoolSafety.gov was created by the federal government to provide schools and districts with actionable recommendations to create a safe and supportive learning environment where students can thrive and grow.

REMS serves two critical functions aimed at building preparedness capacity and serve as the primary source of information dissemination for schools, school districts, and IHEs.

The SSAT is designed to help inform your school’s safety and security planning process by taking stock of what security measures and associated supports are in place across your campus, and where you can make improvements to improve the safety and security of your school community.

The National Center for School Safety (NCSS) is focused on improving school safety and preventing school violence.

This mobile app is designed specifically for education agencies. It allows personnel to walk around buildings and grounds and conduct a site assessment.
The Campus Resilience Program Resource Library aims to provide members of the academic community with access to resources, strategies, guidelines, and templates to address a variety of different vulnerabilities and risks.

This library organizes resources according to a specific threat/hazard, and then further categorizes each resource according to its relevant Mission Area, as outlined in the Federal Emergency Management Agency’s (FEMA) National Preparedness Goal.

- Power Failure
- Cyber Incidents
- Hazardous Materials Release
- School and Workplace Violence
- Explosives Attack
- Epidemic/Pandemic
- Radiological Attack
- Natural Disasters

The Resource Library is currently available in soft launch mode only. Additional resources are being added on an ongoing basis.
Every day, the United States consumes a vast amount of energy. This energy dependence augments the threat of a catastrophic power failure given that even temporary or minor failures interrupt critical economic, communication, and security systems.

Mission Focus Areas:

• **Prevention**: This mission area focuses on the ability to avoid, prevent, or stop an imminent threat.

• **Protection**: This mission area focuses on the ability to secure and protect a community against a variety of threats and hazards.

• **Mitigation**: This mission area focuses on the ability to reduce the loss of life and property by lessening the impact of a disaster
## Resources: Active Assailants

<table>
<thead>
<tr>
<th>Publications</th>
<th>Videos</th>
<th>Other Materials</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Shooter Preparedness In-Person Workshops</td>
<td>Options for Consideration Active Shooter Preparedness Video</td>
<td>Active Shooter Booklet, Quick Reference Guide, Poster, Pocket Card</td>
</tr>
<tr>
<td>Vehicle Ramming Self-Assessment Tool</td>
<td>Vehicle Ramming Attack Mitigation Video</td>
<td>Active Shooter Recovery Guide</td>
</tr>
<tr>
<td>High School Active Shooter CTEP Situation Manual</td>
<td>Active Shooter Emergency Action Planning Video</td>
<td>Recovering from an Active Shooter Incident Fact Sheet</td>
</tr>
<tr>
<td>Middle School Active Shooter CTEP Situation Manual</td>
<td>Template and Guide for Creating an Emergency Action Plan</td>
<td></td>
</tr>
<tr>
<td>Elementary School Active Shooter CTEP Situation Manual</td>
<td>First Responder Toolbox</td>
<td></td>
</tr>
<tr>
<td>K-12 Education Active Threat CTEP Situation Manual</td>
<td>Active Shooter Emergency Action Plan Guide</td>
<td></td>
</tr>
<tr>
<td>Higher Education IED Threat CTEP Situation Manual</td>
<td>CISA Exercises (dhs.gov) (HSIN Account Needed)</td>
<td></td>
</tr>
</tbody>
</table>

Visit: [www.dhs.gov/active-shooter-preparedness](http://www.dhs.gov/active-shooter-preparedness) for more information
Resources: Pathway to Violence

As a follow-on product to the “Power of Hello”, the Cybersecurity and Infrastructure Security Agency (CISA) has developed the **De-Escalation Series** to assist Critical Infrastructure Owners and Operators to recognize the warning signs for someone on the pathway to violence, assess if the situation is escalating, de-escalate the situation currently taking place, and report the situation through organizational reporting if needed and 9-1-1 if the situation is becoming violent or someone is in danger.

Knowing what to say and what to do, can make a big difference and prevent a potential threat!

**RECOGNIZE**

**ASSESS**

**DE-ESCALATE**

**REPORT**

---

**Employee Vigilance and De-escalation | CISA**

**Pathway to Violence Video | CISA**

---

**DHS Violence Prevention Resource Guide**

---

**Pathway to Violence fact sheet**
Resources: Insider Threat Mitigation

- Insider threat incidents are possible in any sector or organization.
- An insider threat is typically a current or former employee, third-party contractor, or business partner.
- In their present or former role, the person has or had access to an organization’s network systems, data, or premises, and uses their access (sometimes unwittingly).
- To combat the insider threat, organizations can implement a proactive, prevention-focused mitigation program to detect and identify threats, assess risk, and manage that risk - before an incident occurs.
- The key steps to mitigate insider threat are Define, Detect and Identify, Assess, and Manage.

For more information on insider threat mitigation, please send an email to InTmitigation@cisa.dhs.gov
Resources: Workplace Violence

• As defined by the U.S. Department of Labor, “a workplace violence incident is a verbal, written, or physically aggressive threat or attack intended to intimidate, cause injury or death to others in a place of employment”.

• The General Duty Clause, Section 5(a)(1) of the Occupational Safety and Health Act directs employers to provide a place of employment that is “free from recognized hazards that are causing or are likely to cause death or serious harm”.

• The resources listed below can assist organizations to better understand workplace violence and develop protective measures.

  - Department of Labor Workplace Violence Program
  - Occupational Safety and Health Administration (OSHA) Workplace Violence Program
  - Occupational Safety and Health Administration (OSHA) Fact Sheet: Workplace Violence
  - FBI Workplace Violence: Issues in Response
  - FBI Workplace Violence Prevention: Readiness and Response
Today we face a variety of threats, both internal and external, from hostile governments, terrorist groups, disgruntled employees and malicious introducers. Alert employees can spot suspicious activity and report it. The power is in the employee, citizen, patron, or any person who can observe and report.

Used effectively, the right words can be a powerful tool. Simply saying “Hello” can prompt a casual conversation with unknown individuals and help you determine why they are there. The OHNO approach – Observe, Initiate a Hello, Navigate the Risk, and Obtain Help – helps employees observe and evaluate suspicious behaviors, and empowers them to mitigate potential risk, and obtain help when necessary.
Public gatherings and crowded places are increasingly vulnerable to terrorist attacks and other extremist actors because of their relative accessibility and large number of potential targets.

Organizations of all types of sizes, including businesses, critical infrastructure owners and operators, schools, and houses of worship face a variety of security risks.

For more information on insider threat mitigation, please send an email to InTmitigation@cisa.dhs.gov
The DHS “If You See Something, Say Something®” Campaign is a national campaign that raises public awareness of:

- the indicators of terrorism and terrorism-related crime; and
- the importance of reporting suspicious activity to state and local law enforcement.

DHS has pre-made materials, such as posters and social media graphics, to help academic campuses raise awareness among its students and employees.

Contact SeeSay@hq.dhs.gov to obtain these materials and learn more.
Resources: Bombing Prevention and Awareness

Resources for:

- **Individuals**
  - DHS-DOJ Bomb Threat Guidance, Bomb Threat Procedures Checklist, What You Can Do When There is a Bomb Threat Video, Bombing Prevention Lanyard Cards

- **First Responders, Military, Government, and Security Personnel**
  - Technical Resource for Incident Prevention (TRIPwire) information sharing network

- **Sports and Entertainment Venues**
  - Sports and Entertainment Venues Bombing Prevention Solutions Portfolio

- **Communities**
  - Multi-Jurisdictional Improvised Explosive Device Security Planning Program

Visit [www.dhs.gov/what-to-do-bomb-threat](http://www.dhs.gov/what-to-do-bomb-threat) for more information
The use of a vehicle as a weapon in a terrorist attack is not new. Recent terrorist incidents and violent extremist propaganda demonstrate that the use of vehicles as a weapon continues to be of interest by those wishing to cause harm.

Attacks of this nature require minimal capability but can have a devastating impact in crowded places with low levels of visible security.

- Vehicle Ramming Self-Assessment Tool
- Self-Assessment Tool Resources
- First Responder Toolbox
- General Resources
- Videos

Vehicle Ramming Self-Assessment Tool
CISA.ISD.OSP.VehicleRammingMitigation@cisa.dhs.gov
Unmanned aircraft systems (UAS), also known as drones, can be used for malicious purposes. These resources provide an overview of the threat and steps businesses, the public, and first responders can take to protect against the malicious use of drones.

<table>
<thead>
<tr>
<th>Publications</th>
<th>Videos</th>
<th>Other Materials</th>
</tr>
</thead>
<tbody>
<tr>
<td>UAS: Addressing Critical infrastructure Security Challenges</td>
<td>UAS Critical Infrastructure Video</td>
<td>UAS Critical infrastructure Drone Pocket Card</td>
</tr>
<tr>
<td>UAS: Considerations for Law Enforcement</td>
<td></td>
<td>UAS: Frequently Asked Questions (website)</td>
</tr>
<tr>
<td>Responding to Drone Calls: Guidance for Emergency Communications Centers</td>
<td></td>
<td>DHS CUAS Legal Authorities</td>
</tr>
</tbody>
</table>

**Resources: Unmanned Aircraft Systems (UAS)**

**Publications**
- UAS: Addressing Critical infrastructure Security Challenges
- UAS: Considerations for Law Enforcement
- Responding to Drone Calls: Guidance for Emergency Communications Centers

**Videos**
- UAS Critical Infrastructure Video

**Other Materials**
- UAS Critical infrastructure Drone Pocket Card
- UAS: Frequently Asked Questions (website)
- DHS CUAS Legal Authorities

**UAS - Critical Infrastructure | CISA**
### Resources: Facility Access

- Resources for screening patrons before allowing them to enter facilities or employing a credentialing process

<table>
<thead>
<tr>
<th>Publications</th>
<th>Videos</th>
<th>Other Materials</th>
</tr>
</thead>
<tbody>
<tr>
<td>**Venue Bag Search Procedures Guide</td>
<td>CISA**</td>
<td><strong>Check It! – Bag Check</strong></td>
</tr>
<tr>
<td><strong>Evacuation Planning Guide for Stadiums</strong></td>
<td><strong>Access and Functional Needs, What you should know</strong></td>
<td>**Counter-IED Awareness Products</td>
</tr>
</tbody>
</table>

**Commercial Facilities Publications | CISA**

**2020 Edition - Facility Access Control: An Interagency Security Committee Best Practice | CISA**
Training provides practitioners the requisite knowledge and skills to respond effectively to an emergency, and exercises test how they manage the response to an incident.
Resources: Critical Infrastructure Security and Resilience Stakeholder Training and Exercises

CISA’s wide array of free training programs provide government officials and critical infrastructure owners and operators with the knowledge and skills needed to implement critical infrastructure security and resilience activities.

• Web-based independent study courses,
• Instructor-led courses
• Associated training materials

CISA Tabletop Exercise Package (CTEP) is a comprehensive set of resources to assist stakeholders in conducting their own customizable tabletop exercises

CISA Training | CISA

Critical Infrastructure Training | CISA

website: CISA Tabletop Exercises Packages | CISA
Exercise Starter Kits (ESK) are self-conducted tabletop exercises (TTX) tailored for the academic community. Topics include:

- Exercise Conduct Briefing
- Situation Manual
- Facilitator Guide

Available within each ESK are the following customizable templates:

- Participant Feedback Form
- After-Action Report Template

Click HERE for more information
Upcoming Events: NATIONAL SUMMIT ON K-12 SCHOOL SAFETY & SECURITY 1-3 NOVEMBER 2022

MISSION
The Summit supports the safety and security of schools by:

- **Fostering a nationwide dialogue** by bringing together stakeholders for exchange, discussion, and connection.
- **Facilitating action** by coordinating and disseminating resources, products, and tools to support schools in implementing and strengthening their security postures.
- **Equipping stakeholders** with training and expertise to apply recognized best practices and research in the context of their specific communities, venues, and schools.

ISSUE AREAS
The Summit program focuses on the safety and security topics of:

- Cybersecurity
- Physical Security
- Emergency Planning
- Capacity Building
- Training, Exercise & Drills
- Targeted Violence
- Reporting Systems
- Threat Assessment
- Capacity Building
- Targeted Violence
- Reporting Systems
- Threat Assessment

WHO SHOULD ATTEND?
Designed for school safety leaders:

- K-12 Educators
- School and District Administrators
- Principals and Superintendents
- School-Based Law Enforcement
- First Responders
- Safety & Security Professionals
- Elected Officials
- Community Liaisons
- Mental Health Professionals
- Government Partner

Registration opened on Wednesday August 24, 2022.

https://www.cisa.gov/national-school-safety-summit
Upcoming Events: CISA ACTIVE SHOOTER WEBINAR

- The Cybersecurity and Infrastructure Security Agency, Region 1 (Connecticut, Massachusetts, Maine, New Hampshire, Rhode Island, Vermont) invites you to join a two-hour security webinar to enhance awareness of and response to an active shooter event on **Wednesday, September 21, 2022, 1:00 p.m. EDT**

- Preparing employees for a potential active shooter incident is an integral component of an organization’s incident response planning. Because active shooter incidents are unpredictable and evolve quickly, preparing for and knowing what to do in an active shooter situation can be the difference between life and death. Every second counts.

- Objectives:
  - Registration for this event is free.
  
  - **Register** or visit [https://www.eventbrite.com/e/cisa-active-shooter-preparedness-webinar-region-1-ctmamenhrvtnrt-registration-391241723527](https://www.eventbrite.com/e/cisa-active-shooter-preparedness-webinar-region-1-ctmamenhrvtnrt-registration-391241723527)

  - Registration is limited to 350 participants and will close no later than 20 September 2022 at noon (12:00 p.m.) EDT
Our Team

Within each CISA Region are your local and regional Protective Security Advisors (PSAs), Cybersecurity Advisors (CSAs), Chemical Inspectors and other CISA personnel. These field personnel advise and assist in training and exercising some of the best practices to supporting our partners in achieving more robust resilience.
Protective Security Advisors (PSA)

• Field-based as critical infrastructure security specialists
• Serve as state, local, tribal, and territorial government and private sector link to CISA resources:
  • Conduct and coordinate assessments, training, and other DHS products and services
  • Provides a vital link for information sharing in steady state and incident response
  • Assist facility owners/operators with obtaining security clearances
  • During contingency events, PSAs support the response, recovery, and reconstitution efforts of States
PSA Assessments

• Assist Visits
• Security at First Entry (SAFE)
• Infrastructure Survey Tool
• Infrastructure Visualization Platform (IVP)
• Multi-Asset & Systems Assessment (MASA)
• Regional Resiliency Assessment Program

Self Assessment Tools

School Security Assessment Tool (SSAT) | CISA
CISA - Active Vehicle Barrier Selection Tool
Vehicle Ramming Self-Assessment Tool:
Houses of Worship | CISA
The CSA mission is to promote cybersecurity preparedness, risk mitigation, and incident response capabilities of public and private sector owners and operators of critical infrastructure, as well as SLTT bodies, through stakeholder partnerships and direct assistance activities.

In support of that mission: Cybersecurity Advisors (CSAs):

- **Assess**: Evaluate critical infrastructure cyber risk.
- **Promote**: Encourage best practices and risk mitigation strategies.
- **Build**: Initiate, develop capacity, and support cyber communities-of-interest and working groups.
- **Educate**: Inform and raise awareness.
- **Listen**: Collect stakeholder requirements.
- **Coordinate**: Bring together incident support and lessons learned.
The Cybersecurity and Infrastructure Security Agency offers a range of cybersecurity assessments that evaluate operational resilience, cybersecurity practices, organizational management of external dependencies, and other key elements of a robust and resilient cyber framework.
CISA recommends all organizations—regardless of size—adopt a heightened posture when it comes to cybersecurity and protecting their most critical assets.

**Reduce the likelihood of a damaging cyber intrusion**
- MFA
- Up to Date Software
- Prioritize KEVs
- Validate Remote Access

**Take steps to quickly detect a potential intrusion**
- Timely assessment of unexpected/unusual network behavior
- Logging

**Ensure that the organization is prepared to respond if an intrusion occurs**
- Designate a crisis-response team
- TTX
- Scalability

**Maximize the organization’s resilience to a destructive cyber incident**
- Test backup procedures
- For ICS, conduct a test of manual controls
Chemical Security Inspectors (CSI)

CSI as part of the Cybersecurity and Infrastructure Security Agency (CISA) serves as Sector Risk Management Agency (SRMA) for the Chemical Sector. The Cybersecurity and Infrastructure Security Agency (CISA) serves as Sector Risk Management Agency (SRMA) for the Chemical Sector. The SRMA works with companies to develop tools and resources for assessing facility security and resilience. CISA also collaborates with public and private sector partners to ensure that chemical facility owners and operators receive important information about human-made and natural threats and hazards that pose the greatest risk to the Nation’s critical chemical facilities.

In support of that mission Protective Security Advisors PSAs):

• **Chemical** Facility Anti-Terrorism Standards (CFATS) regulation compliance
• **Authorization** Inspections (AIs)
• **Compliance** Assistance Visits (CAVs)
• **Comprehensive** Compliance Inspections (CCIs) and Supplemental Compliance Inspections (SCIs)
• **Stakeholder** Outreach
More than 96% of all manufactured goods depend on chemicals in some way. These chemicals are used, manufactured, stored, and transported across global supply chains, forming the bedrock of industries that touch nearly every aspect of American life—from microchips to food processing. Many of these chemicals that businesses interact with every day are dangerous chemicals that could be used in a terrorist attack.

Whether a small business or an international company, everyone who interacts with these chemicals has a role to play in understanding the risk and taking collective action to prevent chemicals being weaponized by terrorists. CISA’s ChemLock program is a completely voluntary program that provides facilities that possess dangerous chemicals no-cost services and tools to help them better understand the risks they face and improve their chemical security posture in a way that works for their business model.

To request any of CISA ChemLock’s no-cost services and tools, please fill out the ChemLock Services Request Form.
The PCII Program

**Purpose** A *nationwide* program supporting DHS, other Federal Agencies, and SLTT governments to *encourage* critical infrastructure (CI) owners in private and SLTT sectors to *voluntarily* submit critical infrastructure information (CII) to the government.

**Protections** Protects Critical Infrastructure Stakeholders from the *federal government*
- Disclosing information through the Freedom of Information Act (FOIA)
- Disclosing information through State & Local Government Disclosure Laws
- Using in Civil Actions
- Using in Regulatory Proceedings

**Authorities**
- Critical Infrastructure Information (CII) Act of 2002
- DHS Management Directive 262-08, PCII Program (2016)

**Duration** Protections have *no* time limit; can be withdrawn by submitter
Contacting Your CT CISA Team

Bryan Gran
Protective Security Advisor, Region I (CT)
Cybersecurity and Infrastructure Security Agency (CISA)
bryan.gran@cisa.dhs.gov

Daniel J. W. King
Chief of Cybersecurity, Region 1 (New England)
Cybersecurity and Infrastructure Security Agency
daniel.king@cisa.dhs.gov

cisa.isd.osp_active_assailant_security@cisa.dhs.gov

Todd Nichols
Chemical Security Inspector, Region 1 (New England)
Cybersecurity and Infrastructure Security Agency (CISA)
todd.nichols@cisa.dhs.gov
Questions?

For additional Information or if you would like to learn more about CISA offerings Email: bryan.gran@cisa.dhs.gov

Or Email CISA Active Assailant @ cisa.isd.osp_active_assailant_security@cisa.dhs.gov

Subscribe today to receive new products on Active Assailant Security

PSA Bryan Gran
August 25, 2022