U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Connecticut Center for School Safety and Crisis Preparation
Western Connecticut State University

PSA Bryan Gran
August 26, 2022

Today’s Agenda

A guide to today's discussion

- Our Work
- CISA and School Safety
- Risk and Emerging Threats
- Security Planning
- Our Resources
- Training and Exercises
- Our Team
- Closing and Questions

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

VISION Secure and resilient infrastructure for the American people.

MISSION We lead the National effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

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 Gol 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** | **GovDelivery 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

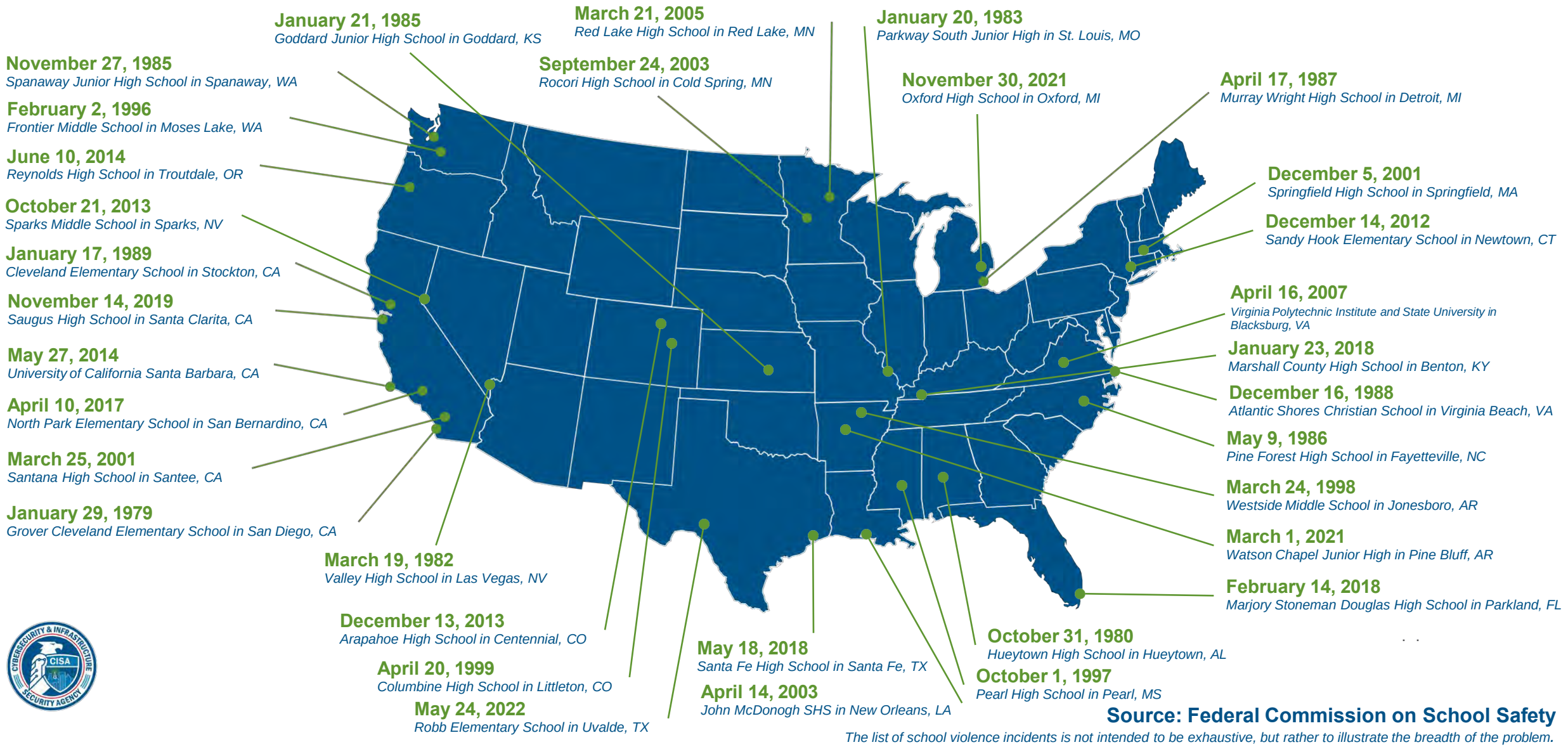
Educational Organizations & Associations
School Safety Organizations
Communities with School Violence Experience
School Safety Conferences

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



Source: Federal Commission on School Safety

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

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

Threat Landscape

- 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.

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

Common Challenges Schools Face

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)
- Funding (Initial, Long Term)
- Seeking Approval (Administration, Board)
- Use and Effectiveness of Measures
- Understanding Limitations (Physical, CRCL, Technology)

SECTION 4.0

COMMON CHALLENGES AND TRADEOFFS IN SCHOOL PHYSICAL SECURITY PLANNING

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. In addition to thinking through what is in place and what gaps exist at each layer, they will also need to think about things such as costs associated with various measures, the extent to which physical security measures adhere to code and comply with state- and local-level school safety policies, and how the measures they put in place might degrade an otherwise welcoming school climate or have differential impacts on diverse segments of their student body.

4.1 | POLICIES

Many policies, statutes, and regulations pertaining to school safety exist at the federal, state, and local levels; making sure that a school is adhering to them can be a challenge, especially for local education agencies who are not experts in security (Steiner et al., 2021).

TABLE 4.1 - TYPES OF PHYSICAL SECURITY POLICIES AT THE FEDERAL, STATE, AND LOCAL LEVELS

	Federal Policy	State Policy	Local Policy
Statutes and Regulations	✓	✓	✓
Guidance	✓	✓	✓
Funding	✓	✓	
Codes		✓	✓

SOURCE: Steiner et al., 2021

At the federal level, a number of statutes and regulations exist to protect the rights of individuals. The Fourteenth Amendment, the Civil Rights Act (Pub. L. 88-352, 1964, as amended and codified), the Family Educational Rights and Privacy Act (FERPA) (Pub. L. 93-380, 1974, § 513), and the Americans with Disabilities Act (ADA) (Pub. L. 101-336, 1990) are all examples of federal laws that local education agencies should consider when planning, selecting, and implementing their physical security system. To avoid installing measures or putting in place measures that might violate the rights of individual students, teachers, and staff, schools should consider these and other regulations in their planning process. Carefully laid out policies and procedures to dictate the use of security measures, as well as communication with the school community about the use and intended purpose of measures, can work to mitigate against unintended adverse consequences in this area.

Regulations that govern school physical security are enacted largely at the state level, and there is considerable variance in policy across states (see e.g. Ehlenberger, 2002). States commonly develop guidance specific to these statutes and regulations, and many also outline best practices related to physical security. While they employ a range of strategies to disseminate this guidance, it is common for state-level agencies involved with school safety to host websites that point local education agencies to specific state-level requirements, as well as to guidance from the federal government, other states, or non-governmental agencies that they deem relevant and useful.

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY | K-12 SCHOOL SECURITY GUIDE | 3rd Edition 24 of 27

Security Plan Development

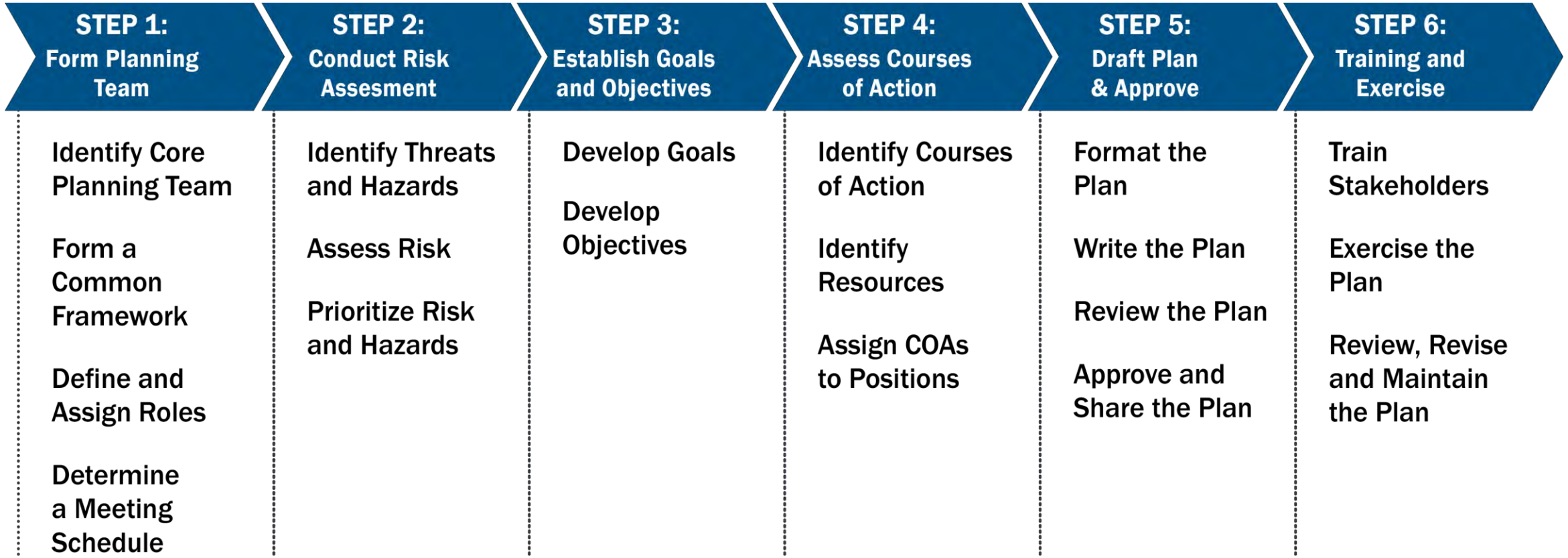
The knowledge of how to plan is critical in emergency of a disaster, including saving lives and protecting property, and helping a community recover more quickly from a disaster.

Cycle of Preparedness

Recognition	Prevention	Protection	Mitigation	Response	Recovery
Form Planning Team	Conduct Risk Assessment	Establish Goals and Objectives	Assess Courses of Action	Draft Plan and Approve	Training and Exercise
· Incident Analysis · Mission Areas · Planning Principles · Planning Team	· Pathway to Violence · Report Behavior · Work Place Violence · Risk Issues	· Site Vulnerabilities · Physical Security · Internal Factors · Goals and Objectives	· Reduce Impact · Communications · Develop Courses of Action · Format Plan	· Steps to Save Lives · Response Coordination · Disability Planning · Approve the plan	· Short-Term Recovery · Long-Term Recovery · Continuity of Operations/ Continuity of Goverment · Training and Exercises
					
Team Identified	**Risks Identified**	**Goals/Objectives Defined**	**Courses of Action Identified**	**Plan Outlined**	**Plan Implemented**

The Planning Process

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.



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

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

FIGURE 2.4 - STEPS IN THE SCHOOL SECURITY PHYSICAL PLANNING PROCESS

STEP 1.
FORM A PHYSICAL SECURITY PLANNING TEAM
Identify and include relevant school staff and stakeholders, such as community organizations, local law enforcement, and families.

STEP 2.
GATHER RELEVANT LOCAL DATA
Gather local data about safety incidents at schools and the consequences of such events.

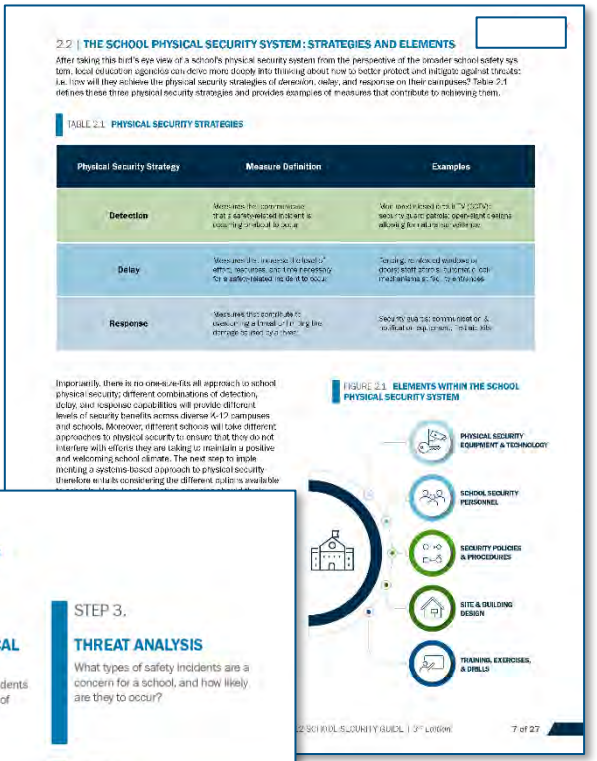
STEP 3.
THREAT ANALYSIS
What types of safety incidents are a concern for a school, and how likely are they to occur?

STEP 4.
VULNERABILITY ANALYSIS
What safety and security measures are already in place at the school?

STEP 5.
RISK ANALYSIS
What are the potential consequences of each of the identified safety incidents based on the security measures in place at the school? How do security measures reduce risk? What risk remains?

STEP 6.
CREATE A SECURITY PLAN
Which of those remaining risks are a concern, and what are the most practical and effective additional safety and security measures to address them?

SOURCE: Adapted from Steiner et al., 2021.



2.2 | THE SCHOOL PHYSICAL SECURITY SYSTEM: STRATEGIES AND ELEMENTS

TABLE 2.1 PHYSICAL SECURITY STRATEGIES

Physical Security Strategy	Measure Definition	Examples
Detection		
Delay		
Response		

FIGURE 2.1 ELEMENTS WITHIN THE SCHOOL PHYSICAL SECURITY SYSTEM

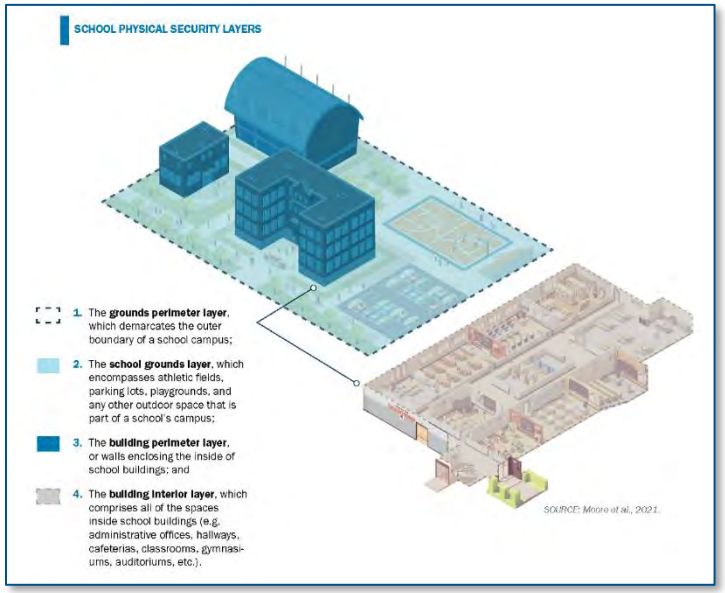
PHYSICAL SECURITY EQUIPMENT & TECHNOLOGY
SCHOOL SECURITY PERSONNEL
SECURITY POLICIES & PROCEDURES
SITE & BUILDING DESIGN
TRAINING, EXERCISES, & DRILLS

Planning-The Security Annex

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

Physical Security Across Layers



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 or 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.

- **Connect**
- **Plan**
- **Train**
- **Report**

For more information on insider threat mitigation, please send an email to InTmitigation@cisa.dhs.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.

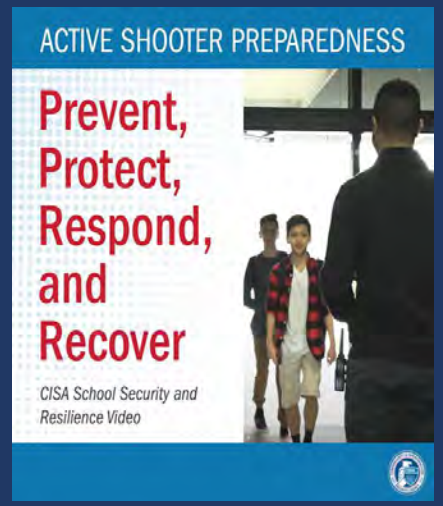
Be Vigilant!

www.dps.mn.gov- The Minnesota School Safety Center

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
- Hometown Security
- School Safety and Security
- Campus Resilience
- Active Assailants
- Pathway to Violence
- Insider Threats
- Workplace Violence
- The Power of Hello
- Pathway to Violence
- Securing Public Gatherings
- Raising Awareness
- Bombing Prevention
- Vehicle Ramming
- UAVs and Facility Access



Products/Resources | CISA

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.

- CP3
- CISA
- FEMA
- Office of Intel and Analysis
- United States Secret Service
- CT Fusion Center
- CT Emergency Management

DHS Violence Prevention Resource Guide | Homeland Security

Resources: Connecticut Intelligence Center

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:** he 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

Resources: Division of Emergency Management and Homeland Security

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

Resources: School Safety and Security

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

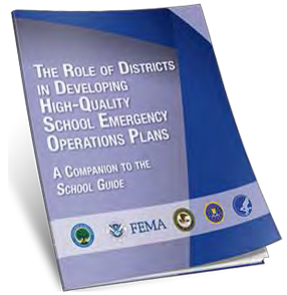
Resources: School Safety and Security

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.

Resources: Campus Resilience Program Resource Library

- 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

DHS Grants

DHS Campaigns

Other Federal Programs and Resources

Additional Resources

The Resource Library is currently available in soft launch mode only. Additional resources are being added on an ongoing basis.

Resources: Campus Resource Library-Power Failure

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

Power Protection

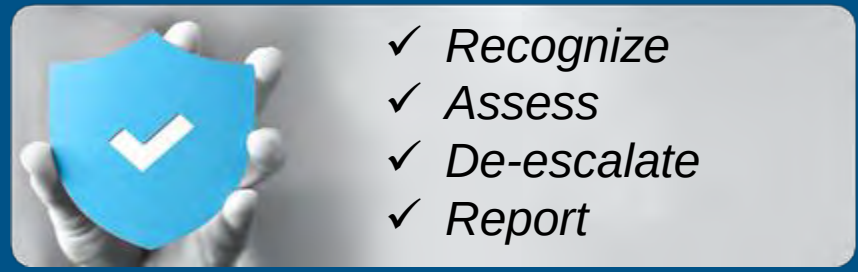
- Cameras & Recording
- Access Control
- Fire Alarm Systems
- Emergency Communications
- Telephone Systems
- Intrusion Detection
- Loss Prevention

Resources: Active Assailants

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

Visit: 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**

DHS Violence Prevention Resource Guide

Employee Vigilance and De-escalation | CISA

Pathway to Violence Video | CISA

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**.

- New Product Alert: The Insider Threat Mitigation Workshop and One-Pager
- The Insider Risk Mitigation Program Evaluation (IRMPE) Assessment Instrument
- Keys to a Successful Insider Threat Mitigation Program
- Insider Threat Videos
- Resources
- Contact Information

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

Resources: The Power of Hello

- 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.

Observe

Initiate a Hello

Navigate the Risk

Obtain Help

Resources

Employee Vigilance - Power of Hello | CISA

Resources: Securing Public Gaterings

- 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.

Securing Public Gatherings Postcard

Suspicious or Unattended Item

Business Continuity and Preparedness

Election Security

Identify Suspicious Behavior

Prepare and Respond to Active Assailants

Prevent and Respond to Bombings

Protect Against Small Unmanned Aircraft Systems

Safeguard and Secure Cyberspace

Prepare for and Respond to Vehicle Ramming Attacks

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

Raising Awareness on Campus

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 Awarness

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 for more information

Resources: Vehicle Ramming Attack Mitigation

- 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

Resources: Unmanned Aircraft Systems (UAS)

- 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

Publications	Videos	Other Materials
UAS: Addressing Critical infrastructure Security Challenges	UAS Critical Infrastructure Video	UAS Critical infrastructure Drone Pocket Card
UAS: Considerations for Law Enforcement		UAS: Frequently Asked Questions (website)
Responding to Drone Calls: Guidance for Emergency Communications Centers		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

Publications	Videos	Other Materials
Venue Bag Search Procedures Guide | CISA	Check It! – Bag Check	Commercial Facilities Resources
Evacuation Planning Guide for Stadiums	Access and Functional Needs, What you should know	Counter-IED Awareness Products | CISA
Commercial Facilities Publications | CISA		

2020 Edition - Facility Access Control: An Interagency Security Committee Best Practice | CISA

Training and Exercises

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.

Training

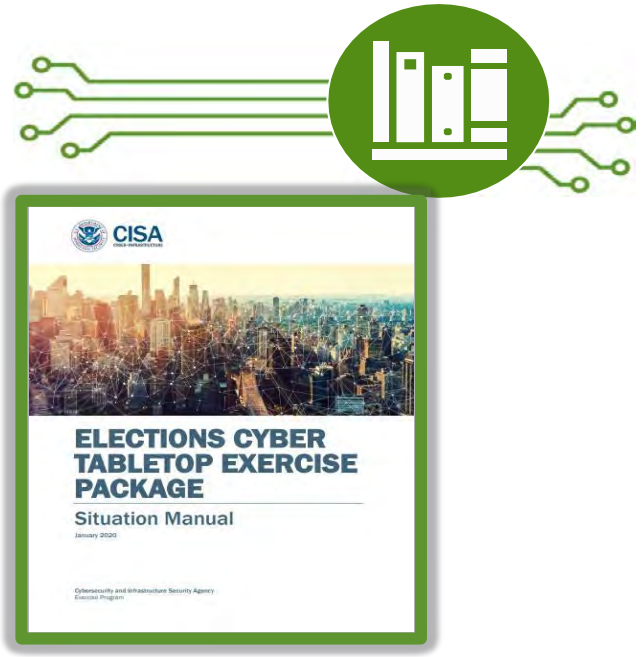
Exercises

Upcoming Training/Events

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

Exercise Starter Kits (ESK) are self-conducted tabletop exercises (TTX) tailored for the academic community. Topics include:


Improvised Explosive Device


Tornado


Hazardous Material Release


Cyber Breach


Earthquake


Active Shooter

Available within each ESK are the following customizable templates:

- Exercise Conduct Briefing
- Situation Manual
- Facilitator Guide
- 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
- Emergency Planning
- Training, Exercise & Drills
- Reporting Systems
- Physical Security
- Capacity Building
- Targeted Violence
- 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- ctmamenhrivt-registration-391241723527**

- **Registration is limited to 350 participants and will close no later than 20 September2022at 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
- Assessments
- Cybersecurity Advisors
- Resources
- Shields Up
- Chemical Inspectors
- ChemLock
- PCII

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

Table 2 Facility and SAA Vulnerabilities and Options for Consideration

Category	Vulnerability	Option(s) for Consideration
Facility		
Security Management Profile	The facility's security plan is missing key elements.	Update the security plan to include the following: • Security force – Roving patrols[i]
Security Management Profile	Although the facility conducts background checks on employees, checks are conducted only at initial hire. Recurring background checks are not conducted.	• Conduct recurring background check on employees.[ii]
Security Management Profile	Although background checks are conducted on contactors personnel, checks are conducted only at initial hire. Recurring background checks are not conducted.	• Ensure recurring background checks are conducted on contractors as appropriate. For example, recurring background checks may be necessary for contractors working in positions of trust or assigned to critical or sensitive areas. Recurring background checks may occur on an annual basis, randomly, or on special occasions (e.g., when an contractor is eligible for reassignment).[iii]
Security Management Profile	Background checks are not conducted on vendors.	• Require vendors to conduct background checks on their personnel who will work at the facility. Obtain proof from vendors that appropriate background checks have been conducted.[iv]
Resilience Management Profile	The facility trains some, but not all, personnel on the emergency action/emergency operations plan.	• Train all personnel on emergency procedures for life safety at least once a year.

Self Assessment Tools

School Security Assessment Tool (SSAT) | CISA

CISA - Active Vehicle Barrier Selection Tool

Vehicle Ramming Self-Assessment Tool:

Houses of Worship | CISA

Cybersecurity Advisors (CSA)

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.

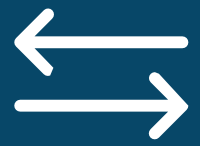
CISA CYBER Resources

CYBERSECURITY | CISA

The Cybersecurity and Infrastructure Security Agency offers arrange 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.

Assessments & Services

Cyber Resilience Review	Phishing Campaign Assessment
Cyber Infrastructure Survey	Remote Penetration Testing
Vulnerability Scanning	Validated Architecture Design Review
Web Application Scanning	Risk and Vulnerability Assessment



Resources

National Cyber Awareness System	Federal Cyber Incident & Vulnerability Playbooks	Known Exploited Vulnerabilities Catalog
Stuff Off Search	Bad Practices	And More...

SHIELDS UP

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

Resources: Chemical Security

ChemLock

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.

ChemLock | CISA

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.

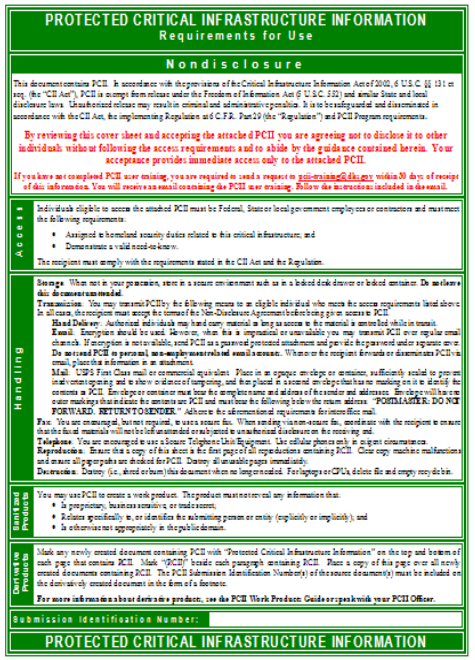
Protections Protects Critical Infrastructure Stakeholders from the ***federal government***

- 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
- 6 Code of Federal Regulations part 29 (2006) (Tech Edits in FY22)
- PCII Program Procedures Manual (2009) (Updating)
- DHS Management Directive 262-08, PCII Program (2016)

Duration Protections have no time limit; can be withdrawn by submitter



PROTECTED CRITICAL INFRASTRUCTURE INFORMATION
Requirements for Use

Nondisclosure

This document contains PCII. In accordance with the provisions of the Critical Infrastructure Information Act of 2002, 6 U.S.C. §§ 131 et seq. (the "CII Act"), PCII is exempt from release under the Freedom of Information Act (5 U.S.C. 552) and similar State and local disclosure laws. Unauthorized release may result in criminal and administrative penalties. It is to be safeguarded and disseminated in accordance with the CII Act, the implementing Regulation at 6 C.F.R. Part 29 (the "Regulation") and PCII Program requirements.

By reviewing this cover sheet and accepting the attached PCII you are agreeing not to disclose it to other individuals without following the access requirements and to abide by the guidance contained herein. Your acceptance provides immediate access only to the attached PCII.

If you have not completed PCII user training, you are required to send a request to pcii-training@dhs.gov within 30 days of receipt of this information. You will receive an email containing the PCII user training. Follow the instructions included in the email.

Access

Individuals eligible to access the attached PCII must be Federal, State or local government employees or contractors and must meet the following requirements:

- Assigned to homeland security duties related to this critical infrastructure; and
- Demonstrate a valid need-to-know.

The recipients must comply with the requirements stated in the CII Act and the Regulation.

Handling

Storage: When not in your possession, store in a secure environment such as in a locked desk drawer or locked container. Do not leave this document unattended.

Transmission: You may transmit PCII by the following means to an eligible individual who meets the access requirements listed above. In all cases, the recipient must accept the terms of the Non-Disclosure Agreement before being given access to PCII.

Hand Delivery: Authorized individuals may hand carry material as long as access to the material is controlled while in transit.

Email: Encryption should be used. However, when this is impractical or unavailable you may transmit PCII over regular email channels. If encryption is not available, send PCII as a password protected attachment and provide the password under separate cover. Do not send PCII to personal, non-employer controlled email accounts. Whenever the recipient forwards or disseminates PCII via email, place this information in an attachment.

Mail: USPS First Class mail or commercial equivalent. Place in an opaque envelope or container, sufficiently sealed to prevent inadvertent opening and to show evidence of tampering, and then placed in a second envelope that has no marking on it to identify the contents as PCII. Envelope or container must bear the complete name and address of the sender and addressee. Envelope will have no outer marking that indicate the contents are PCII and must bear the following below the return address: "POSTMASTER: DO NOT FORWARD. RETURN TO SENDER." Adhere to the aforementioned requirements for interoffice mail.

Fax: You are encouraged, but not required, to use a secure fax. When sending via non-secure fax, coordinate with the recipient to ensure that the faxed materials will not be left unattended or subjected to unauthorized disclosure on the receiving end.

Telephone: You are encouraged to use a Secure Telephone Unit/Equipment. Use cellular phones only in exigent circumstances.

Reproduction: Ensure that a copy of this sheet is the first page of all reproductions containing PCII. Clear copy machine malfunctions and ensure all paper jams are cleared for PCII. Destroy all unusable pages immediately.

Destruction: Destroy (i.e., shred or burn) this document when no longer needed. For laptops or CPUs, delete file and empty recycle bin.

Sanitized Products

You may use PCII to create a work product. The product must not reveal any information that:

- Is proprietary, business sensitive, or trade secret;
- Relates specifically to, or identifies the submitting person or entity (explicitly or implicitly); and
- Is otherwise not appropriately in the public domain.

Derivative Products

Mark any newly created document containing PCII with "Protected Critical Infrastructure Information" on the top and bottom of each page that contains PCII. Mark "(PCII)" beside each paragraph containing PCII. Place a copy of this page over all newly created documents containing PCII. The PCII Submission Identification Number(s) of the source document(s) must be included on the derivatively created document in the form of a footnote.

For more information about derivative products, see the PCII Work Product Guide or speak with your PCII Officer.

Submission Identification Number:

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

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

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

cisa.isd.osp_active_assailant_security@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***