Community Support Resources

- **Protective Security Advisors**: Physical security subject matter experts located across the country who conduct security assessments, provide access to security guidance, training, and exercises, and advise on enhanced protective measures.
- **Cybersecurity Advisors**: Cybersecurity subject matter experts located across the country who conduct security assessments, provide access to security guidance, training, and exercises, and advise on enhanced protective measures.

- Security and Resilience Resources for At-Risk Communities: builds security capacity of the public and private sector to mitigate a wide range of threats including active shooters, vehicle ramming, insider threats, and small unmanned aircraft systems.
  - Securing Public Gatherings
  - Mass Gathering Security Planning Tool
  - Protecting Infrastructure During Public Demonstrations

  - **Targeted Violence Prevention**
    - Pathway to Violence: Warning Signs and What You Can Do
    - Power of Hello
    - Personal Security Considerations
    - Mitigating the Impacts of Doxing

  - Active Shooter Preparedness**:** a comprehensive set of courses, materials, and workshops that better prepare you to deal with an active shooter situation, focusing 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.
    - Active Shooter Preparedness Webinar
    - Planning and Response to an Active Shooter Guidance
    - Active Shooter Preparedness: Access & Functional Needs – What You Should Know Video
    - Translated Active Shooter Preparedness Resources

  - Vehicle Ramming Mitigation**:** provides mitigation tools for terrorist attacks when a vehicle is used as a weapon.
    - Vehicle Ramming Self-Assessment Tool
    - Vehicle Ramming Action Guide
    - Active Vehicle Barrier Selection Tool
    - Guide to Active Vehicle Barrier Specification and Selection Resources

  - Insider Threat Mitigation**:** explains the key steps to mitigate insider threat: Define, Detect and Identify, Assess, and Manage.
    - Insider Threats 101 Fact Sheet
    - Insider Risk Mitigation Program Evaluation Self-Assessment Tool

  - **Bombing Prevention Resources:** builds capability within the general public and across the public and private sectors to prevent, protect against, respond to, and mitigate bombing incidents.

    - Bombing Prevention landing page: Bombing Prevention | Cybersecurity and Infrastructure Security Agency CISA
    - Bomb threat resources: Bomb Threats | CISA
    - Specific resources for Universities and College Campuses:
        - ✓ Bomb Threat Guide – Comprehensive guide developed to assist Decision Makers plan for, assess, and respond to bomb threats in an orderly and controlled manner.
        - ✓ Bomb Threat Procedures & Checklist – Reference checklist that provides instructions on how to respond to a bomb threat in addition to a comprehensive list of information that will assist law enforcement in a bomb threat investigation.
        - ✓ Suspicious or Unattended Item – Reference postcard that provides a process to determine if an item is a serious threat or just unattended.
        - ✓ Bomb Threat Stand-Off – Quick reference postcard providing recommended evacuation and shelter-in-place distances for various types and sizes of IEDs.
        - ✓ Mass Bomb Threats – Postcard that provides awareness on mass bomb threat campaigns. Illustrates their impacts and indicators with a focus on evaluating risk levels and threat response options.
        - ✓ Bomb Threat Management Annex Template | CISA - Assists college and university officials charged with developing and implementing plans to manage bomb threat situations. It contains definitions, quick reference guides, planning considerations, and template language to simplify the task of developing safe and effective response procedures.
        - ✓ What to Do: Bomb Threat – Demonstrates procedures to follow when receiving a bomb threat and will help individuals prepare and react appropriately.

- **School Safety Resources:** builds the capacity of schools and districts to protect against and mitigate security threats and risks.
    - K-12 School Security Guide Product Suite, a comprehensive set of doctrine and resources designed to provide K-12 districts and campuses with resources, tools, and strategies to improve school physical security. The suite outlines action-oriented practices and helps schools and districts learn the steps necessary to assess vulnerabilities, strengthen security, and better protect against a range of targeted violence and other threats.
    - K-12 School Security Guide and School Security Assessment Tool, a web-based assessment that walks users through a tailorable vulnerability analysis and provides results and recommendations that can be integrated into a school's existing safety and security plans.
    - CISA-USSS K-12 Bystander Reporting Toolkit, which is designed to strengthen school safety reporting programs and encouraging bystander reporting among students and other members of the school community. Developed in partnership with the USSS NTAC, the toolkit offers simple strategies and guidance to implement or enhance safety reporting programs and create a school environment where students are more willing and able to report concerns for the wellness and safety of themselves or others.

- **CISA Exercises Resources:** CISA Exercises offers the following exercise services to the academic community, including K-12 and higher education:

- Exercise Planning and Conduct Support Services, Exercise Planning and Conduct, CISA designs, develops, conducts, and evaluates exercises ranging from small-scale, limited-scope, discussion-based exercises (e.g., two-hour seminars) to large-scale, operations-based exercises (e.g., multi-day, full-scale exercises). Scenarios cover an array of cybersecurity and physical security threats ranging from ransomware to active shooters and improvised explosive devices (IEDs).
- CISA Tabletop Exercise Packages (CTEPs), CTEPs are a comprehensive set of resources designed to assist stakeholders in conducting their own exercises and initiating discussions within their organizations about their ability to address a variety of threat scenarios. CTEPs are customizable and include templated exercise objectives, scenarios, discussion questions, and a collection of references and resources.
  - ➢ CISA has over 100 total CTEPs available on CISA.gov, including seven specific to the academic community. Specifically:
    - ✓ K-12 Schools Cyber, Elementary School Active Shooter, Higher Education Active Threat, Higher Education Improvise Explosive Device, High School Active Shooter, K-12 Active Threat, and Middle School Active Threat.

Information Sharing

- Technical Resource for Incident Prevention (TRIPwire)**:** online portal that combines up-to-date threat information and security resources specific to bombing incidents to help users anticipate, identify, and prevent bombing-related incidents.
- Federal School Safety Clearinghouse Main Page**:** provides schools and districts with actionable recommendations to create a safe and supportive learning environment for students and educators. The site serves as a one-stop shop access point for information, resources, guidance and evidence-based practices on a range of school safety topics and threats, including violence prevention.

Training

- Bombing Prevention Training and Resources: CISA's Office for Bombing Prevention offers bombing prevention training throughout the United States on multiple platforms to meet stakeholder needs, including direct-delivery, in-person in a traditional classroom setting or in-residence at the Federal Emergency Management Agency's Center for Domestic Preparedness, online through a Virtual Instructor-Led Training (VILT) platform, and through Independent Study Training.
  - Training Recommendations for All School Employees:
    - Bomb Threat Preparedness and Response (AWR-903) – One-hour online independent study training to familiarize participants with the steps necessary to prepare for and respond to a bomb threat.
    - Response to Suspicious Behaviors and Items (AWR-335) – One-hour Virtual Instructor-Led Training (VILT) introduces participants to recognizing and responding to suspicious behaviors, activities, and items related to terrorist or criminal activities.
  - Bombing Prevention training recommendations for school administrators and security:

        - Bomb Threat Assessment for Decision Makers (AWR-945) – One-hour VILT introduces the participant to types of threats, the threat assessment process, and the implementation of a bomb threat management (BTM) plan.
        - Bomb Threat Management (BTM) Planning (MGT-451) – One-day Instructor-Led Training (ILT) provides participants with foundational knowledge of the Department of Homeland Security's risk management process and BTM planning.
        - Improvised Explosive Device (IED) Search Procedures (PER-339) – One-day ILT introduces participants to basic, low-risk search protocols. It provides participants with the information needed to create a search plan for their facility or special event. It provides them guidance on how to perform IED searches of a route, area, and a facility.

- **Active Shooter:** instructor-led and online training modules, as well as resources, focused on behavioral indicators, emergency action plan creation, actions that may be taken to increase probability of survival, and how to quickly recover from an incident. Resources are available in multiple languages. What You Can Do Online Training.

    - Active Shooter Options for Consideration Training Video**:** demonstrates possible actions to take if confronted with an active shooter scenario. The video also shows how to assist authorities once law enforcement enters the scene.

- Defusing Potentially Violent Situations**:** provide a description of methods, such as purposeful actions and verbal communications, to prevent potential violence or dangerous situations.

Cybersecurity Resources

- Malicious cyber actors are targeting K–12 education organizations across the country, with potentially catastrophic impacts on students, their families, teachers, and administrators. A new report from the Cybersecurity and Infrastructure Security Agency (CISA) helps schools reduce the risks of a cyber catastrophe.
    - CISA, "Protecting our Future: Cybersecurity for K-12," https://www.cisa.gov/protecting-our-future-cybersecurity-k-12. Last accessed July 28, 2023.
- Based on feedback from K–12 stakeholders, CISA offers the following recommendations to help K–12 leaders build, operate, and maintain resilient cybersecurity programs.
    - **Recommendation 1:** Invest in the Most Impactful Security Measures and Build Toward a Mature Cybersecurity Plan.
        - Multifactor Authentication, CISA
        - Phishing-Resistant MFA Fact Sheet, CISA
        - Cyber Hygiene Services, CISA
        - Known Exploited Vulnerabilities Catalog, CISA
        - Get Your Stuff Off Search, CISA
        - Cross-Sector Cybersecurity Performance Goals, CISA
        - CPGs Checklist, CISA
        - Nationwide Cybersecurity Review (NCSR), CISA
        - Cybersecurity Framework, NIST
        - Cybersecurity Considerations for K–12 Schools and School Districts, Readiness and Emergency Management for Schools (REMSTA)

        - Ransomware Guide (September 2020), CISA
        - K12 SIX Essential Cyber Incident Response Runbook (June 22, 2022), K12 SIX
        - State Cybersecurity Best Practices Incident Response Plan (Fall 2022), State Educational Technology Directors Association
    - **Recommendation 2:** Recognize and Actively Address Resource Constraints.
        - Free Cybersecurity Services and Tools, CISA
        - FY22 State and Local Cybersecurity Grant Program Fact Sheet, CISA
        - State and Local Cybersecurity Grant Program Frequently Asked Questions, CISA
        - Homeland Security Grant Program, FEMA
        - Homeland Security Grant Program (HSGP) Application Process, FEMA
    - **Recommendation 3:** Focus on Collaboration and Information Sharing.
        - Join MS-ISAC — Free for U.S. State, Local, Tribal & Territorial Government Entities, Center for Internet Security (CIS)
        - Report to CISA, CISA
        - Internet Crime Complaint Center (IC3), FBI
    - Training for K-12 Students and Educators
        - Federal Virtual Training Environment (FedVTE) Public Courses
        - Foundations of Cybersecurity for Managers, National Initiative for Cybersecurity Careers and Studies (NICCS)
        - Fundamentals of Cyber Risk Management, NICCS
        - Don't Wake Up to a Ransomware Attack, NICCS
        - SchoolSafety.gov Cybersecurity Topic Page
        - Cybersecurity Training and Exercises, CISA
        - NICCS Education and Training Catalog
        - CETAP Cyber Safety Videos, Cyber.org and CISA Counselors
        - Cybersecurity Considerations for K–12 Schools and School Districts, REMS-TA Center
        - The Largest Cybersecurity Hacking Competition
- CISA recommends that the Education Facilities Subsector should leverage mitigations and follow the Department of Education's Resources for K-12 Districts and Higher Education Institutions.
    - A Parent's Guide for Understanding K-12 School Data Breaches: Resource for parents of K-12 students to help understand what it means when a school has a data breach, as well as provides tools and best practices to help navigate the sometimes-confusing process of protecting students' data in the event of a breach.
    - Addressing Adversarial and Human Caused Threats That May Impact Students, Staff, and Visitors: Resource helps plan for adversarial- and human-caused threats, such as cyber safety and cybersecurity, within K-12 schools and institutions of higher education.
    - Building Technology Infrastructure for Learning Guide: Resource provides practical, actionable information to help school and district leaders (including superintendents, principals, and senior technology staff) navigate the many decisions required to build a technology infrastructure that supports digital learning.
    - Cyber Safety Quick Links for Protecting Youth: Empowering Students to Become Responsible Digital Citizens and Engage Online Safely: Resource gives families, students, and school safety teams key practical steps and quick links to Websites offering free

cyber safety resources, tools, and training.

  - Cybersecurity Community of Practice: Forum for schools, school districts, institutions of higher education (IHEs), and community partners to collaborate, share, and learn from the experiences of others in the field.
  - Cybersecurity Considerations for K-12 Schools and School Districts: Resource focuses on addressing threats to a school's or school district's network and systems.
  - Data Breach Response Checklist: Resource includes a thorough checklist based on best practices from the National Institute of Standards and Technology (NIST), US-CERT, and other industry thought leaders to assist schools to evaluate and build strong incident response processes and plans to their unique requirements.
  - Data Breach Scenario Training Kits: Resource includes packaged trainings developed by the Privacy Technical Assistance Center, designed to help educational organizations at all levels conduct internal staff development on data breaches.
  - Data Security and Monitoring Training Best Practices: Resource provides best practices for data security and data management trainings for educational leaders and discusses key training concepts to follow, content, delivery methods, and possible audiences for these trainings.
  - Data Security Checklist: Resource assists stakeholder organizations with developing and maintaining a successful data security program by listing essential components that should be considered when building such a program, with focus on solutions and procedures relevant for supporting data security operations of educational agencies.
  - Dear School Safety Partner: Cybersecurity and Cyber Safety: Resource provides information on cybersecurity for schools as well as steps education agencies can take, with the collaboration of parents, to protect student privacy while increasing the use of digital learning and video sharing platforms in response to the COVID-19 pandemic.
  - Integrating Cybersecurity with EOPs for K-12 Schools: Webinar focuses on the importance of cybersecurity and network protection for schools.

Contacts

- CISA Central**:** mechanism for critical infrastructure stakeholders to engage with CISA; a simplified entry point for stakeholders to request assistance. Contact directly via Central@cisa.gov.
- CISA Regional Offices **(including Protective and Cyber Security Advisors):** executes mission objectives during steady-state and incident operations; provides local and facility-based support to critical infrastructure stakeholders. Contact directly via:
- **Region 1** (Maine, New Hampshire, Vermont, Massachusetts, Rhode Island, and Connecticut): CISARegion1@hq.dhs.gov
- **Region 2** (New York, New Jersey, Puerto Rico, and Virgin Islands): CISARegion2@hq.dhs.gov
- **Region 3** (Pennsylvania, West Virginia, Maryland, Delaware, Virginia, and the District of Columbia): CISARegion3@hq.dhs.gov
- **Region 4** (Kentucky, Tennessee, North Carolina, South Carolina, Mississippi, Alabama, Georgia, and Florida): CISARegion4@hq.dhs.gov

- **Region 5** (Ohio, Michigan, Indiana, Illinois, Wisconsin, and Minnesota): CISARegion5@hq.dhs.gov
- **Region 6** (Louisiana, Arkansas, Oklahoma, Texas, and New Mexico): CISARegion6@hq.dhs.gov
- **Region 7** (Missouri, Kansas, Nebraska, and Iowa): CISARegion7@hq.dhs.gov
- **Region 8** (Colorado, Utah, Wyoming, Montana, North Dakota, and South Dakota): CISARegion8@hq.dhs.gov
- **Region 9** (Arizona, Nevada, California, Guam, American Samoa, Commonwealth of Northern Mariana Islands, and Hawaii): CISARegion9@hq.dhs.gov
- **Region 10** (Washington, Oregon, Idaho, and Alaska): CISARegion10@hq.dhs.gov