CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY STAKEHOLDER RESOURCES & CONTACTS

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (CISA) STAKEHOLDER RESOURCES & CONTACTS

Sign up for Alerts: https://public.govdelivery.com/accounts/USDHSCISA/subscriber/new?qsp=CODE_RED

REPORT A CYBERSECURITY INCIDENT: REPORT ANOMALOUS CYBER ACTIVITY AND/OR CYBER INCIDENTS 24/7 TO REPORT@CISA.GOV OR (888) 282-0870.

- Report an Incident
- Report Phishing
- Report a Vulnerability

CONTACT US: HTTPS://WWW.CISA.GOV/ABOUT/CONTACT-US

CISA LEADERSHIP

CISA	Director	Deputy Director	Executive Director
	Jen Easterly	Nitin Natarajan	Brandon Wales
	Executive Assistant Director	**Deputy Executive Assistant Director**	
CSD	Jeff Greene	Mathew Hartman	
ECD	Bill Bob Brown Jr	Vincent Delaurentis	
ISD	Dr. David Mussington	Steve Harris	
	Assistant Director	**Deputy Assistant Director**	
IOD	Bridgette Bean	Boyden Rohner	
NRMC	Mona Harrington	Jennifer Pedersen (A)	
SED	Trent Frazier	Ryan Donaghy (A)	

STAKEHOLDER ENGAGEMENT DIVISION - STRATEGIC RELATIONS

HQ	Associate Director	Deputy Associate Director	Partnership's Branch Chief
STRATEGIC RELATIONS	Kevin Dillon kevin.dillon@cisa.dhs.gov	Sara Pease sara.pease@cisa.dhs.gov	Bob Nadeau robert.nadeau@cisa.dhs.gov

REGIONAL CONTACTS

<table>
<tr><th>Region</th><th>Regional Director</th><th>Deputy Regional Director</th><th>Executive Officer</th></tr>
<tr><td>Region 1</td><td>Matthew McCann</td><td>Tom Filippone</td><td>Tracy Shawyer</td></tr>
<tr><td colspan="4">Contacts
Regional office: CISARegion1@cisa.dhs.gov
Media inquiries: CISAMedia@cisa.dhs.gov
After hours: Central@cisa.gov
To report anomalous cyber activity and/or cyber incidents 24/7, email report@cisa.gov, or 1-844-Say-CISA (1-844-729-2472).</td></tr>
<tr><td>Region 2</td><td>John Durkin</td><td>Mohammad Telab</td><td>Kelly Quinones</td></tr>
<tr><td colspan="4">Contacts
Regional office: CISARegion2@cisa.dhs.gov
Media inquiries: CISAMedia@cisa.dhs.gov
After hours: Central@cisa.gov
To report anomalous cyber activity and/or cyber incidents 24/7, email report@cisa.gov, or 1-844-Say-CISA (1-844-729-2472).</td></tr>
<tr><td>Region 3</td><td>William Ryan</td><td>James Cratty</td><td>Deadra Sotero- Long</td></tr>
<tr><td colspan="4">Contacts
Regional office: CISARegion3@cisa.dhs.gov
Media inquiries: CISAMedia@cisa.dhs.gov
After hours: Central@cisa.gov
To report anomalous cyber activity and/or cyber incidents 24/7, email report@cisa.gov, or 1-844-Say-CISA (1-844-729-2472).</td></tr>
<tr><td>Region 4</td><td>Julius Gamble</td><td>Kate Nichols</td><td>Noah Goulding</td></tr>
<tr><td colspan="4">Contacts
Regional office: CISARegion4@cisa.dhs.gov
Media inquiries: CISAMedia@cisa.dhs.gov
After hours: Central@cisa.gov
To report anomalous cyber activity and/or cyber incidents 24/7, email report@cisa.gov, or 1-844-Say-CISA (1-844-729-2472).</td></tr>
<tr><td>Region 5</td><td>Alex Joves</td><td>Kathryn Young</td><td>Beth Windisch</td></tr>
<tr><td colspan="4">Contacts
Regional office: CISARegion5@cisa.dhs.gov
Media inquiries: CISAMedia@cisa.dhs.gov
After hours: Central@cisa.gov
To report anomalous cyber activity and/or cyber incidents 24/7, email report@cisa.gov, or 1-844-Say-CISA (1-844-729-2472).</td></tr>
</table>

<table>
<tr><td>Region 6</td><td>Robert Russell (A)</td><td>Bryan Gray (A)</td><td>Ricardo Gonzalez</td></tr>
<tr><td colspan="4">Contacts
Regional office: CISARegion6@cisa.dhs.gov
Media inquiries: CISAMedia@cisa.dhs.gov
After hours: Central@cisa.gov
To report anomalous cyber activity and/or cyber incidents 24/7, email report@cisa.gov, or 1-844-Say-CISA (1-844-729-2472).</td></tr>
<tr><td>Region 7</td><td>Phil Kirk</td><td>Ethan Cole</td><td>Steven Marin</td></tr>
<tr><td colspan="4">Contacts
Regional office: CISARegion7@cisa.dhs.gov
Media inquiries: CISAMedia@cisa.dhs.gov
After hours: Central@cisa.gov
To report anomalous cyber activity and/or cyber incidents 24/7, email report@cisa.gov, or 1-844-Say-CISA (1-844-729-2472).</td></tr>
<tr><td>Region 8</td><td>Shawn Graff</td><td>Joseph O’Keefe</td><td>Andre Mouton</td></tr>
<tr><td colspan="4">Contacts
Regional office: CISARegion8@cisa.dhs.gov
Media inquiries: CISAMedia@cisa.dhs.gov
After hours: Central@cisa.gov
To report anomalous cyber activity and/or cyber incidents 24/7, email report@cisa.gov, or 1-844-Say-CISA (1-844-729-2472).</td></tr>
<tr><td>Region 9</td><td>David Rosado</td><td>Frank Calvillo</td><td>Christopher Fiorenza</td></tr>
<tr><td colspan="4">Contacts
Regional office: CISARegion9@cisa.dhs.gov
Media inquiries: CISAMedia@cisa.dhs.gov
After hours: Central@cisa.gov
To report anomalous cyber activity and/or cyber incidents 24/7, email report@cisa.gov, or 1-844-Say-CISA (1-844-729-2472).</td></tr>
<tr><td>Region 10</td><td>Patrick Massey</td><td>Barret Adams-Simmons</td><td></td></tr>
<tr><td colspan="4">Contacts
Regional office: CISARegion10@cisa.dhs.gov
Media inquiries: CISAMedia@cisa.dhs.gov
After hours: Central@cisa.gov
To report anomalous cyber activity and/or cyber incidents 24/7, email report@cisa.gov, or 1-844-Say-CISA (1-844-729-2472).</td></tr>
</table>

RESOURCES

Secure Our World – CISA's New National Cybersecurity Awareness Program: https://www.cisa.gov/secure-our-world
Staying Safe Online is Easier Than You Think! We're increasingly connected through digital tools and more of our sensitive information is online. This convenience comes with risks. Each of us has a part to play in keeping ourselves and others safe. It's easy to do and takes less time than you think! See all the new resources CISA has developed so that we can all take steps everyday to reduce on-line risk.

Active Shooter Pocket Card | CISA: https://www.cisa.gov/resources-tools/resources/active-shooter-pocket-card
The Active Shooter Pocket Card offers suggestions about how a bystander should react in an active shooter situation.

Best Practices: https://www.cisa.gov/topics/cybersecurity-best-practices
CISA provides information on cybersecurity best practices to help individuals and organizations implement preventative measures and manage cyber risks.

Cloud Environment Factsheet of Free Tools:
https://www.cisa.gov/news-events/alerts/2023/07/17/cisa-develops-factsheet-free-tools-cloud-environments
CISA has developed and published a factsheet, Free Tools for Cloud Environments, to help businesses transitioning into a cloud environment identify proper tools and techniques necessary for the protection of critical assets and data security. Free Tools for Cloud Environments provides network defenders and incident response/analysts open-source tools, methods, and guidance for identifying, mitigating, and detecting cyber threats, known vulnerabilities, and anomalies while operating a cloud or hybrid environment.

CISA Gateway: https://www.cisa.gov/resources-tools/services/cisa-gateway
The CISA Gateway serves as the single interface through which DHS partners can access a large range of integrated infrastructure protection tools and information to conduct comprehensive vulnerability assessments and risk analysis.

CISA Services: https://www.cisa.gov/resources-tools/services
A searchable database of services offered by CISA.

CISA Strategic Plan: https://www.cisa.gov/cybersecurity-strategic-plan
The *FY2024-2026 Cybersecurity Strategic Plan* guides CISA's efforts in pursuit of a new vision for cybersecurity: a vision grounded in collaboration, in innovation, and in accountability.
Aligned with the National Cybersecurity Strategy and nested under CISA's 2023–2025 Strategic Plan, the Cybersecurity Strategic Plan provides a blueprint for how the agency will pursue a future in which damaging cyber intrusions are a shocking anomaly, organizations are secure and resilient, and technology products are secure by design and default. To this end, the Strategic Plan outlines three enduring goals:

- Address Immediate Threats by making it increasingly difficult for our adversaries to achieve their goals by targeting American and allied networks;
- Harden the Terrain by adopting strong practices for security and resilience that measurably reduce the likelihood of damaging intrusions; and
- Drive Security at Scale by prioritizing cybersecurity as a fundamental safety issue and ask more of technology providers to build security into products throughout their lifecycle, ship products with secure defaults, and foster radical transparency into their security practices so that customers clearly understand the risks they are accepting by using each product.

CISA Training: https://www.cisa.gov/cybersecurity-training-exercises
CISA looks to enable the cyber-ready workforce of tomorrow by leading training and education of the cybersecurity workforce by providing training for federal employees, private-sector cybersecurity professionals, critical infrastructure operators, educational partners, and the general public. CISA is committed to supporting the national cyber workforce and protecting the nation's cyber infrastructure.

CISA TTX Packages: https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages
CISA Tabletop Exercise Packages (CTEPs) are a comprehensive set of resources designed to assist stakeholders in conducting their own exercises. Partners can use CTEPs to initiate discussions within their organizations about their ability to address a variety of threat scenarios.

Cyber Hygiene Services & Vulnerability Scanning Services: https://www.cisa.gov/cyber-hygiene-services
Adversaries use known vulnerabilities and phishing attacks to compromise the security of organizations. CISA offers scanning and testing services to help organizations reduce their exposure to threats by taking a proactive approach to mitigating attack vectors. Email us at vulnerability@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services" to get started.

Cyber Guidance for Small Businesses: https://www.cisa.gov/cyber-guidance-small-businesses
We offer an action plan for small businesses that is informed by the way cyber-attacks actually happen, that lays the groundwork for building an effective security program.

Cross Sector Cybersecurity Performance Goals: https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
Developed in coordination between CISA, the National Institute of Standards and Technology (NIST), and the interagency community, these voluntary cross-sector Cybersecurity Performance Goals (CPGs) are intended to help establish a common set of fundamental cybersecurity practices for critical infrastructure, and especially help small- and medium-sized organizations kickstart their cybersecurity efforts.

Communications and Cyber Resiliency Toolkit: https://www.cisa.gov/resources-tools/resources/communications-and-cyber-resiliency-toolkit
CISA developed the Public Safety Communications and Cyber Resiliency Toolkit to assist public safety agencies and others responsible for communications networks in evaluating current resiliency capabilities, identifying ways to improve resiliency, and developing plans for mitigating the effects of potential resiliency threats.

Cybersecurity Education & Career Development: (https://www.cisa.gov/topics/cybersecurity-best-practices/cybersecurity-education-career-development)
Cybersecurity professionals are critical - in both private industry and the government - to the security of individuals and the nation. CISA is committed to strengthening the nation's cybersecurity workforce through standardizing roles and helping to ensure we have well-trained cybersecurity workers today as well as a strong pipeline of future cybersecurity leaders.

Cybersecurity Awareness Month (October) Resources and Toolkit: https://www.cisa.gov/cybersecurity-awareness-month (email: AwarenessCampaigns@cisa.dhs.gov)
Since 2004, the President of the United States and Congress have declared October to be Cybersecurity Awareness Month, helping individuals protect themselves online as threats to technology and confidential data become more commonplace. CISA and the National Cybersecurity Alliance (NCA) lead a collaborative effort between government and industry to raise cybersecurity awareness nationally and internationally.

Decider Fact Sheet: https://www.cisa.gov/resources-tools/resources/decider-fact-sheet
On March 1, 2023, CISA released Decider, a free tool to help the cybersecurity community map threat actor behavior to the MITRE ATT&CK framework. Created in partnership with the Homeland Security Systems Engineering and Development Institute™ (HSSEDI) and MITRE, Decider helps make mapping quick and accurate through guided questions, a powerful search and filter function, and a cart functionality that lets users export results to commonly used formats. CISA encourages the community to use the tool in conjunction with the recently updated Best Practices for MITRE ATT&CK® Mapping guide.

Cybersecurity Toolkit and Resources to Protect Elections: https://www.cisa.gov/cybersecurity-toolkit-and-resources-protect-elections
CISA has compiled a toolkit of free services and tools intended to help state and local government officials, election officials, and vendors enhance the cybersecurity and cyber resilience of U.S. election infrastructure. This toolkit includes free tools, services, and resources provided by CISA, JCDC members, and the cybersecurity community.

Emergency Communications: https://www.cisa.gov/topics/emergency-communications
CISA provides plans, resources, and training to support emergency communications for first responders.

Emergency Communications Awareness Month (April): https://www.cisa.gov/emergency-communications-month
Through its emergency communications mission, CISA conducts extensive, nationwide outreach to support and promote the ability of emergency response providers and government officials to be able to communicate in the event of a natural disaster, terrorist act, or other hazard. CISA also provides guidance on how facilities can establish protocols for identifying and reporting significant cyber incidents to appropriate facility personnel, local law enforcement, and the agency.

Free Cybersecurity Services and Tools: https://www.cisa.gov/free-cybersecurity-services-and-tools
As part of our continuing mission to reduce cybersecurity risk across U.S. critical infrastructure partners and state, local, tribal, and territorial governments, CISA has compiled a list of free cybersecurity tools and services to help organizations further advance their security capabilities. This living repository includes cybersecurity services provided by CISA, widely used open-source tools, and free tools and services offered by private and public sector organizations across the cybersecurity community. The list is not comprehensive and is subject to change pending future additions.

Healthcare and Public Health (HPH) Toolkit and Cybersecurity Performance Goals:
https://www.cisa.gov/topics/cybersecurity-best-practices/healthcare
To help improve cybersecurity within the HPH sector, CISA, the Department of Health and Human Services (HHS), and Health Sector Coordinating Council (HSCC) Cybersecurity Working Group are working together to deliver tools, resources, training, and information that can help organizations within this sector. This toolkit consolidates key resources for HPH organizations at every level. In addition, HHS published voluntary healthcare specific Cybersecurity Performance Goals to help healthcare organizations prioritize implementation of high-impact cybersecurity practices.

Homeland Security Information Network- Critical infrastructure: https://www.dhs.gov/hsin-critical-infrastructure
The Homeland Security Information Network (HSIN) is the trusted network for homeland security mission operations to share Sensitive but Unclassified (SBU) information. The Critical Infrastructure community on HSIN (HSIN-CI) is the primary system through which private sector owners and operators, DHS, and other federal, state, and local government agencies collaborate to protect the nation's critical infrastructure.

Infrastructure Security Awareness Month (November): https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/infrastructure-security-month-2022
CISA invites all Americans to remember that Infrastructure Security is National Security. Keeping the nation's critical infrastructure secure is important to our national security, economy and overall way of life. Critical infrastructure spans everything from telecommunications and chemical facilities to healthcare and financial systems and much more. It is interdependent with other critical infrastructure and supporting systems and encompasses all the essential services that keep our country and our economy running.

JCDC News and Resources: https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative/jcdc-news-and-resources
Links to external news sources that highlight relevant cybersecurity information. CISA established JCDC—the Joint Cyber Defense Collaborative—to unify cyber defenders from organizations worldwide. This diverse team proactively gathers, analyzes, and shares actionable cyber risk information to enable synchronized, holistic cybersecurity planning, cyber defense, and response.

K-12 Report: https://www.cisa.gov/K12Cybersecurity
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 CISA helps schools reduce the risks of a cyber catastrophe.
And Toolkit: https://www.cisa.gov/resources-tools/resources/partnering-safeguard-k-12-organizations-cybersecurity-threats-online
To help schools address cybersecurity risks, CISA developed a report with recommended actions and cybersecurity guidelines for leaders in the K-12 community. The report and this corresponding toolkit are designed to help K-12 schools and school districts most effectively reduce their cybersecurity risks.

National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework: (https://www.cisa.gov/national-initiative-cybersecurity-education-nice-cybersecurity-workforce-framework)
The NICE Cybersecurity Workforce Framework is the foundation for increasing the size and capability of the U.S. cybersecurity workforce. It provides a common definition of cybersecurity, a comprehensive list of cybersecurity tasks, and the knowledge, skills, and abilities required to perform those tasks.

National Initiative for Cybersecurity Careers and Studies: (https://niccs.cisa.gov/cybersecurity-career-resources/additional-resources)
NICCS provides cybersecurity-related resources and links provided here for your information and convenience.

Partnerships: (https://www.cisa.gov/topics/partnerships-and-collaboration)
At CISA, partnership and collaboration are our foundation and the lifeblood of what we do. Information sharing and cooperative action – across both public and private sectors – is essential to our goal of raising the nation's collective defense.

Protecting Houses of Worship: Perimeter Security Considerations Infographic:
https://www.cisa.gov/resources-tools/resources/protecting-houses-worship-perimeter-security-considerations-infographic
This resource is a companion piece to CISA's and the Federal Bureau of Investigation's (FBI) co-branded Protecting Places of Worship: Six Steps to Enhance Security Against Targeted Violence Fact Sheet, which highlighted the following steps: understand risk; understand your space; develop and practice a plan; inform and educate greeters; pursue grants; and report hate crimes and other incidents. This infographic outlines low- to no-cost solutions to help implement these suggested practices and highlights ways to identify funding for security improvements. To learn more about layered security and other recommended mitigations, visit CISA's Mitigating Attacks on Houses of Worship Security Guide.

Ransomware Resources: https://www.cisa.gov/stopransomware
Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. These resources are designed to help individuals and organizations prevent attacks that can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services.

Resource Hub: https://www.cisa.gov/cyber-resource-hub
CISA 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. These professional, no-cost assessments are provided upon request on a voluntary basis and can help organizations manage risk and strengthen the cybersecurity of our Nation's critical infrastructure.

School Safety: https://www.cisa.gov/topics/physical-security/school-safety CISA, along with other organizations throughout government, law enforcement, and communities nationwide, supports K-12 schools and districts in their efforts to enhance school safety and security. CISA's School Safety Task Force is the agency's dedicated program established to strengthen schools' safety and security across the country.

Shields Ready: https://www.cisa.gov/shields-ready
CISA's Shields Ready campaign is about making resilience during incidents a reality by taking action before incidents occur. As a companion to CISA's Shields Up initiative, Shields Ready drives action at the intersection of critical infrastructure resilience and national preparedness. This campaign is designed to help all critical infrastructure stakeholders to take action to enhance security and resilience—from industry and businesses to government entities at all levels, and even individuals by providing recommendations, products, and resources to increase individual and collective resilience for different risk contexts and conditions.

State and Local Cybersecurity Grant Program: https://www.cisa.gov/state-and-local-cybersecurity-grant-program
On September 16, 2022, DHS announced a first-of-its-kind cybersecurity grant program specifically for state, local, tribal and territorial (SLTT) governments. Funding from the State and Local Cybersecurity Grant Program (SLCGP) and the Tribal Cybersecurity Grant Program (TCGP) helps eligible entities address cybersecurity risks and threats to information systems owned or operated by—or on behalf of—state, local and territorial (SLLT) governments. Through two distinct Notice of Funding Opportunities (NOFO), SLCGP and TCGP combined will distribute $1 billion over four years to support projects throughout the performance period of up to four years.

Securing Small and Medium-Sized Business (SMB) Supply Chains: A Resource Handbook to Reduce Information and Communication Technology Risks: https://www.cisa.gov/resources-tools/resources/securing-smb-supply-chains-resource-handbook
Developed by the ICT Supply Chain Risk Management (SCRM) Task Force, this handbook provides an overview of the highest supply chain risk categories commonly faced by ICT small and medium-sized businesses (SMBs), including cyber risks, and contains several use cases that can assist ICT SMBs in identifying the necessary resources to implement ICT supply chain security practices.

Secure by Design: https://www.cisa.gov/securebydesign
It's time to build cybersecurity into the design and manufacture of technology products. The cybersecurity burden is placed disproportionately on the shoulders of consumers and small organizations

and away from the producers of the technology and those developing the products that increasingly run our digital lives. Americans need a new model to address the gaps in cybersecurity—a model where consumers can trust the safety and integrity of the technology that they use every day.

Water and Wastewater Infrastructure Security Toolkit and Resources: https://www.cisa.gov/water
This toolkit consolidates key resources for water and wastewater systems at every level of cybersecurity maturity. For organizations that are just starting to develop their cybersecurity strategies, the fundamental cyber hygiene steps are basic, low or no cost steps that every organization and individual should take to improve their security. The toolkit can help water and wastewater systems build their cybersecurity foundation and progress to implement more advanced, complex tools to strengthen their defenses and stay ahead of current threats.

COMMUNITY SUPPORT RESOURCES

Election Security Advisors (ESA): ESAs will build stronger connective tissue between election officials and our team at CISA. These election security advisors will be experts in the space, with firsthand knowledge of and experience with the infrastructure and officials across their regions in order to provide more tailored guidance and support to reduce risk from the full range of cyber and physical threats to election infrastructure.

Emergency Communications Coordinators (ECC): Emergency Communications Coordinators support emergency communications interoperability by offering training, tools, and workshops, and provide coordination and support in times of threat, disruption, or attack. These services assist CISA stakeholders in ensuring they have communications during steady and emergency operations. Through these programs, CISA helps ensure public safety and national security and emergency preparedness communities can seamlessly and securely communicate.

Chemical Security Inspectors (CSI): Chemical Security Inspectors (CSIs) advise and assist facilities with hazardous chemicals on security measures to reduce the risk of those chemicals being weaponized. For facilities covered under the Chemical Facility Anti-Terrorism Standards (CFATS) program, this includes working with the highest-risk chemical facilities to develop security plans and inspecting to ensure that security is in place. For facilities that do not fall under the CFATS program, CSIs facilitate and provide voluntary security resources, including guidance, best practices, and training.

Cybersecurity Advisors (CSA): CSAs are 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.

Protective Security Advisors (PSA): over 170 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.

Physical Security Resources: builds security capacity of 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: https://www.cisa.gov/topics/physical-security/securing-public-gatherings
- Mass Gathering Security Planning Tool: https://www.cisa.gov/resources-tools/resources/mass-gathering-security-planning-tool
- Protecting Infrastructure During Public Demonstrations: https://www.cisa.gov/sites/default/files/publications/Protecting%20Infrastructure%20During%20Public%20Demonstrations_102220_FINAL_508.pdf

Targeted Violence Prevention

- Pathway to Violence: Warning Signs and What You Can Do: https://www.cisa.gov/resources-tools/resources/pathway-violence
- Power of Hello: https://www.cisa.gov/sites/default/files/publications/CISA_Power_of_Hello_SlickSheet.pdf
- Personal Security Considerations: https://www.cisa.gov/sites/default/files/publications/CISA Fact Sheet_Personal Security Considerations_FINAL_508_0.pdf
- Mitigating the Impacts of Doxing: https://www.cisa.gov/sites/default/files/publications/CISA Insight_Mitigating the Impacts of Doxing_508.pdf

Active Shooter Preparedness: https://www.cisa.gov/topics/physical-security/active-shooter-preparedness

- Active Shooter Preparedness Webinar: https://www.cisa.gov/resources-tools/training/active-shooter-preparedness-webinar
- Planning and Response to an Active Shooter Guidance: https://www.cisa.gov/resources-tools/resources/isc-planning-and-response-active-shooter-guide
- Active Shooter Preparedness: Access & Functional Needs – What You Should Know Video: https://www.youtube.com/watch?v=m3-_z1Q1bFg
- Translated Active Shooter Preparedness Resources: https://www.cisa.gov/translated-active-shooter-preparedness-products-and-resources

Vehicle Ramming Mitigation: https://www.cisa.gov/topics/physical-security/vehicle-ramming-mitigation

- Vehicle Ramming Self-Assessment Tool: https://www.cisa.gov/vehicle-ramming-self-assessment-tool
- Vehicle Ramming Action Guide: https://www.cisa.gov/resources-tools/resources/vehicle-ramming-action-guide
- Active Vehicle Barrier Selection Tool: https://www.cisa.gov/resources-tools/resources/active-vehicle-barrier-selection-tool
- Guide to Active Vehicle Barrier Specification and Selection Resources: https://www.cisa.gov/resources-tools/resources/guide-active-vehicle-barrier

Insider Threat Mitigation: https://www.cisa.gov/topics/physical-security/insider-threat-mitigation

- Insider Threats 101 Fact Sheet: https://www.cisa.gov/resources-tools/resources/insider-threat-101-fact-sheet
- Insider Risk Mitigation Program Evaluation Self-Assessment Tool: https://www.cisa.gov/resources-tools/resources/insider-risk-mitigation-program-evaluation-irmpe

Bombing Prevention Resources: https://www.cisa.gov/topics/physical-security/bombing-prevention

- Counter-IED Awareness Products: https://www.cisa.gov/counter-ied-awareness-products/
- What to Do: Bomb Threat Resources: http://www.cisa.gov/what-to-do-bomb-threat
- What to Do: Bomb Threat Video: https://www.youtube.com/watch?v=pg7yVTBciWg
- Bomb Threat Guidance Brochure: https://www.cisa.gov/sites/default/files/publications/Bomb-Threat-Guidance-Quad-Fold.pdf
- Suspicious or Unattended Item Card: https://www.cisa.gov/sites/default/files/publications/Unattended_vs._Suspicious_Item_Postcard_508Compliant.pdf
- What to Do: Suspicious or Unattended Item Video: https://www.youtube.com/watch?v=rl3iJlFTFC0
- Technical Resource for Incident Prevention (TRIPwire): https://www.tripwire.dhs.gov/

TRAINING

Bombing Prevention Training and Resources: https://www.cisa.gov/topics/physical-security/bombing-prevention/office-bombing-prevention-obp-training
Response to Suspicious Behavior and Items Course: https://cdp.dhs.gov/training/course/AWR-335
Surveillance Detection for Bombing Prevention Course Fact Sheet:
https://www.cisa.gov/sites/default/files/publications/PER-346-Fact-Sheet-508-V2.1.pdf
Active Shooter Instructor-led and Online Training Modules: https://www.cisa.gov/resources-tools/training/active-shooter-what-you-can-do
Active Shooter Options for Consideration Training Video:
https://www.youtube.com/watch?v=tq21iSXDBWg
Defusing Potentially Violent Situations: https://www.cisa.gov/sites/default/files/publications/De-Escalation_Final 508 %2809.21.21%29.pdf