Colorado Homeland Security Resources
**Partnership and Information Sharing Resources**

**U.S. Department of Homeland Security (DHS):** Links to information on DHS missions to include preventing terrorism and enhancing security; managing our borders; administering immigration laws; securing cyberspace; and ensuring disaster resilience: [http://www.dhs.gov](http://www.dhs.gov). The link to the DHS Critical Infrastructure Protection page, including many of the Infrastructure Protection Programs, is [https://www.dhs.gov/hometown-security](https://www.dhs.gov/hometown-security). DHS personnel based in Colorado include representatives of DHS’ operational agencies, as well as the Protective Security Advisors (PSAs), Intelligence Officer (IO), and Cybersecurity Advisor (CSA).

**Colorado Division of Homeland Security & Emergency Management (DHSEM):** The mission of the Division of Homeland Security and Emergency Management is to support the needs of local government and partner with them before, during, and after a disaster and to enhance preparedness statewide by devoting available resources toward prevention, protection, mitigation, response and recovery, ensuring greater resiliency of our communities. [http://www.dhsem.state.co.us/](http://www.dhsem.state.co.us/). Resources include the Colorado Information Analysis Center (CIAC), Terrorism Liaison Officer (TLO) Program, Grant Programs, Training and Exercise Program, Field Services, and State Emergency Operations Center. In addition:

- The Business Emergency Operations Center (BEOC) helps facilitate rapid resource mobilization of the private sector to emergencies in the state of Colorado: [https://www.colorado.gov/pacific/cobeoc/](https://www.colorado.gov/pacific/cobeoc/)
- The Colorado School Safety Resource Center (CSSRC) collaboratively assists schools and communities to create safe and positive K-12 and higher education environments. The CSSRC provides consultation, resources, training, and technical assistance to foster safe and secure learning environments, positive school climates, and early intervention to prevent crisis situations. [www.Colorado.gov/CSSRC](http://www.Colorado.gov/CSSRC)

**InfraGard:** The goal of InfraGard is to promote ongoing dialogue and timely communication between members and the FBI. InfraGard members gain access to information that enables them to protect their assets and in turn give information to government that facilitates its responsibilities to prevent and address terrorism and other crimes. [http://www.infragard.net](http://www.infragard.net)

**Colorado Emergency Preparedness Partnership (CEPP):** The mission of the partnership is to strengthen Colorado’s collective capacity to prevent, respond to, and recover from natural and human-caused disasters through effective public-private collaboration. [http://www.thecepp.org/](http://www.thecepp.org/)

**Protected Critical Infrastructure Information Program:** The Protected Critical Infrastructure Information (PCII) Program is an information-protection program that enhances voluntary information sharing between infrastructure owners and operators and the government. PCII protections mean that homeland security partners can be confident that sharing their information with the government will not expose sensitive or proprietary data. [http://www.dhs.gov/protected-critical-infrastructure-information-pcii-program](http://www.dhs.gov/protected-critical-infrastructure-information-pcii-program).

**Homeland Security Information Network (HSIN):** The Homeland Security Information Network (HSIN) is a national, secure, and trusted web-based portal for information sharing and collaboration between Federal, State, local, tribal, territorial, private sector, and international partners engaged in the homeland security mission. HSIN is made up of a growing network of communities called Communities of Interest, including one for Critical Infrastructure and many for various critical infrastructure sectors. To request access to HSIN, please submit the following (Name, Employer, Title, Business email, Brief written justification) to HSIN.Outreach@hq.dhs.gov.

**TRIPwire:** A Web portal designed for law enforcement and critical infrastructure security personnel. TRIPwire provides expert threat analyses, reports, and planning documents to help anticipate, identify, and prevent Improvised Explosive Device (IED) incidents. [https://tripwire.dhs.gov/](https://tripwire.dhs.gov/)

**Private Sector Clearance Program (PSCP):** The majority of information DHS shares with the private sector will be at unclassified or Sensitive but Unclassified levels. However, there will be instances when the information being shared is
deemed classified. When this is the case, it will be necessary for the private sector official to be cleared for a federal security clearance, thereby allowing access to classified information. DHS will decide whether the Federal Government should sponsor an applicant for a security clearance, based on specific criteria. Contact your PSA for further information.

**Community Emergency Response Teams (CERT):** CERT educates individuals about disaster preparedness for hazards that may impact their area and trains them in basic disaster response skills, such as fire safety, light search and rescue, team organization, and disaster medical operations. Using training learned in the classroom and during exercises, CERT volunteers can assist others in their community following a disaster when professional responders are not immediately available to help. CERT volunteers are also encouraged to support emergency response agencies by taking an active role in emergency preparedness projects. [https://www.fema.gov/community-emergency-response-teams](https://www.fema.gov/community-emergency-response-teams)

**Faith Safety Network (FSN):** To address the growing threat of violence at houses of worship, the Faith Safety Network provides free, practical resources to promote safety and security at faith-based venues. Open to all religious institutions, FSN is a source of pertinent, time-critical alerts, as well as an accessible information-sharing platform of best safety practices and expert counsel to its members. [https://faithsafetycolorado.org/](https://faithsafetycolorado.org/)

**Government Emergency Telecommunications System (GETS):** GETS provides emergency access and priority processing in the local and long distance segments of the Public Switched Telephone Network (PSTN). It is intended to be used in an emergency or crisis situation when the PSTN is congested and the probability of completing a call over normal or other alternate telecommunication means has significantly decreased. [http://www.dhs.gov/government-emergency-telecommunications-service-gets](http://www.dhs.gov/government-emergency-telecommunications-service-gets)

#### Planning Resources

**Ready.gov:** A national public service advertising campaign designed to educate and empower Americans to prepare for and respond to emergencies including natural disasters and potential terrorist attacks. Planning resources include personal and business emergency response planning, crisis communication planning, a Business Continuity Planning Suite, and training and exercise planning guidelines.


**Standard Response Protocol:** Courtesy of the *i love u guys* Foundation, the Standard Response Protocol (SRP) offers four simple but specific actions that can be performed during any incident. Execution of the action is performed by active participants, including students, staff, teachers and first responders. [http://www.iloveuguys.org/srp.html](http://www.iloveuguys.org/srp.html)

**Support Anti-terrorism by Fostering Effective Technologies (SAFETY Act):** The SAFETY Act is intended to provide critical incentives for the development and deployment of anti-terrorism technologies by providing liability protections for suppliers and recipients of “qualified anti-terrorism technologies.” [https://www.safetyact.gov/pages/homepages/Home.do](https://www.safetyact.gov/pages/homepages/Home.do)

**Influenza Information:** One-stop access to U.S. Government information on the flu: Symptoms & Treatment; Prevention & Vaccination; Who’s at Risk; About the Flu; Planning & Preparedness; and Pandemic Awareness. [http://www.flu.gov/](http://www.flu.gov/)

**USSS National Threat Assessment Center (NTAC):** You can find school-related information including the following reports: The Final Report and Findings of the Safe School Initiative; Threat Assessment in Schools; and Prior Knowledge of Potential School-Based Violence. [http://www.secretservice.gov/ntac.shtml](http://www.secretservice.gov/ntac.shtml)
Federal Aviation Administration (FAA) No Drone Zone: The FAA is leading a public outreach campaign to promote safe and responsible use of unmanned aircraft systems and offers a free digital toolkit with outreach materials to federal, state, and other partners to educate unmanned aircraft operators that flying in certain areas is prohibited. This toolkit includes No Drone Zone signage for any medium, including print and web. Follow along with the latest regulations and changes at https://www.faa.gov/Dronezone/.

Regional Resiliency Assessment Program (RRAP): DHS has conducted several projects in Colorado that examine the resilience of one or several infrastructure sectors in the given community. Consult your Protective Security Advisor for more information.

Basic Cybersecurity Planning: The STOP. THINK. CONNECT. ™ Campaign is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. Resources for various types of organizations are available at: https://www.dhs.gov/stopthinkconnect-toolkit

Security Assessment Resources

Infrastructure Survey Tool (IST): The IST is a facility assessment that focuses on identifying gaps and providing options for consideration to enhance overall resiliency. The IST uses analysis of critical assets and current security measures via the creation of a math based, updateable Protective Measures Index (PMI), to identify vulnerabilities and develop mitigation strategies. As an outcome to this visit, you will receive a PMI Dashboard that graphically illustrates your facilities' current security posture as well as a written report that highlights our observations, noted vulnerabilities, your commendable actions, and prospective options for consideration. A Rapid Survey Tool (RST) is also available. It examines a facility in less detail within a significantly shorter visit time. The RST is ideal for a single owner to compare the physical security posture of multiple buildings in their purview.

Dependency Analysis / Service Provider Review: Dependency analysis capabilities provide a rapid visual representation of the relationships and dependencies between critical infrastructure sites. Enhancements to these capabilities result in increased knowledge about critical infrastructure dependencies, thereby enabling improved stakeholder support for special event & incident planning and decision-making processes. Survey can be conducted at the facility or service provider level.
Infrastructure Protection Gateway (IP Gateway): A DHS-managed portal available to agencies at all levels of government to streamline infrastructure information sharing. Users can conduct assessments or utilize the analytical tools. To obtain access to the IP Gateway, all users must have a valid need to know, and complete PCII Authorized User training, and complete all follow-on IP Gateway system training. For more information visit [http://www.dhs.gov/ipgateway](http://www.dhs.gov/ipgateway) and contact the State administrator via the CIAC (cdps_ciac@state.co.us).

Infrastructure Visualization Platform (IVP): The IVP is a multimedia tool that creates an interactive visual guide of any location by integrating various types of data. The IVP generates a 360-degree geospherical video and geospatial panoramic imagery of facilities, surrounding areas, transportation routes, and other areas of interest to provide emergency response personnel and infrastructure operators with interactive data, plan, and images.


Guidelines for School Security Self-Assessment: This resource provides information, ideas and guidelines you need to conduct a comprehensive and effective security assessment of your place of worship: [https://www.dhs.gov/publication/k-12-school-security-guide](https://www.dhs.gov/publication/k-12-school-security-guide).

Best Practices for Anti-Terrorism Security (BPATS) for Commercial Office Buildings: A National Institute of Building Sciences program for evaluating a building's security system. This assessment can be included in support of a SAFETY Act application should a building owner chose to seek protections. [https://bpatsassessmenttool.nibs.org/](https://bpatsassessmenttool.nibs.org/)

Cybersecurity Resources

**National Cybersecurity and Communications Integration Center (NCCIC):** The DHS 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement. [https://www.dhs.gov/national-cybersecurity-and-communications-integration-center](https://www.dhs.gov/national-cybersecurity-and-communications-integration-center). NCCIC’s National Cybersecurity Assessment and Technical Services (NCATS) offers cybersecurity scanning and testing services that identify vulnerabilities within stakeholder networks and provide risk analysis reports with actionable remediation recommendations. For more information, email NCATS_Info@DHS.gov.

**Critical Infrastructure Cyber Community Voluntary Program (C³):** The C³ (pronounced “C Cubed”) Voluntary Program assists critical infrastructure with cybersecurity measures by encouraging the adoption of the National Institute of Standards and Technology’s (NIST) Cybersecurity Framework, released in February 2014. [https://www.us-cert.gov/ccubedvp](https://www.us-cert.gov/ccubedvp).

**Cybersecurity Advisor (CSA) Assessments:** CSAs promote resilience of key cyber infrastructure by providing education, assessments and other direct services tailored to an organization’s maturity level. CSAs also provide on-site meetings, educational and awareness briefings, information sharing, and incident support. Request services at cyberadvisor@hq.dhs.gov.

**Multi-State Information Sharing and Analysis Center (MS-ISAC):** The mission of the MS-ISAC is to improve the overall cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery. [https://www.cisecurity.org/ms-isac/](https://www.cisecurity.org/ms-isac/)

**Automated Information Sharing:** International in scope and free for public use, DHS offers three community-driven technical specifications designed to enable automated information sharing for cybersecurity situational awareness, real-time network defense and sophisticated threat analysis. They include TAXII™, the Trusted Automated eXchange of Indicator Information; STIX™, the Structured Threat Information eXpression; and CybOX™, the Cyber Observable eXpression. [https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity](https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity).
FBI – Cyber Crime: The Federal Bureau of Investigation (FBI) leads the national effort to investigate high-tech crimes, including cyber-based terrorism, espionage, computer intrusions, and major cyber fraud. To stay in front of current and emerging trends, they gather and share information and intelligence with public and private sector partners worldwide. http://www.fbi.gov/about-us/investigate/cyber

---

**Online Training Resources**

**FEMA Emergency Management Institute (EMI):** EMI is the national focal point for emergency management training to enhance the capabilities of government officials, volunteer organizations, and the public and private sectors to minimize the impact of disasters on the American public. http://training.fema.gov/EMIWeb//IS/crslist.asp takes you to a list of about 60 independent study courses, many under 3 hours. Examples include: IS-100: Introduction to the Incident Command System (ICS); IS-546: Continuity of Operations (COOP) Awareness Course IS-700: National Incident Management System (NIMS); IS-800: National Response Framework (NRF); IS-860: National Infrastructure Protection Plan (NIPP); and IS-907: Active Shooter, What You Can Do.

**8 Signs of Terrorism Video:** Terrorist operations usually begin with extensive planning. You can help prevent and detect terrorism, and other types of crime, by watching out for suspicious activities and reporting them to the proper authorities. The video, narrated by John Elway, is a partnership between the CELL, CIAC, DHS, and FBI. http://www.youtube.com/watch?feature=player_embedded&v=iWnKvhVnl9U

**Active Shooter Preparedness:** DHS offers free courses, materials, and workshops to better prepare you to deal with an active shooter situation and to raise awareness of behaviors that represent pre-incident indicators and characteristics of active shooters. http://www.dhs.gov/activeshooter. Navigate to “Workshop Participants” to view videos, including Insider Threat videos, for incorporation into your workplace training. Find additional videos made by major city police departments on YouTube.

**Private Sector Cybersecurity Training:** ICS-CERT has web-based courses which focus on control systems and cyber-related threats which are aimed at the private sector. Program and course descriptions are available at: http://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT; while the learning portal is located at: https://ics-cert-training.inl.gov/learn

**Virtual Instructor Led Training (VILT):** VILT courses provide general awareness level protective measures and counter-improvised explosive device (C-IED) information to a broad audience through an on-line virtual training experience with a live instructor. Perfect for participants with time availability constraints, they can be taken as stand-alone courses or serve as prerequisites for many other Office for Bombing Prevention (OBP) courses. https://cdp.dhs.gov/obp

**Critical Infrastructure Tabletop Exercise Program:** Comprehensive sets of templates for exercise planning and conduct that correspond to various scenarios and infrastructure sectors are available on HSIN by searching for “CITEP” or at https://hsin.dhs.gov/ci/sites/exerciseinfo/Pages/CITEP_LearnmoreHome.aspx. More than 20 packages contain fully developed scenarios, presentations, handbooks, and correspondence templates.

---

**Onsite Training Resources**

**Community Awareness Program (CAP):** The Community Awareness Program™ (CAP), hosted in partnership with the Counter-terrorism Education Learning Lab (The CELL) and the Colorado Information Analysis Center (CIAC), empowers citizens to help play a role in enhancing our community’s safety. The CAP is a free, interactive course taught by members of the public safety community. It provides citizens with the basic tools needed to recognize and help prevent criminal activity and terrorism in the United States while preserving civil liberties protected by the U.S. Constitution. http://www.thecell.org/cap/

**Active Shooter Preparedness for Employees:** Protective Security Advisors are available to conduct awareness-level training on active shooter preparedness and survival utilizing the Run – Hide – Fight paradigm.
**Security Awareness and Training focused on Counter-IED:** The DHS Office for Bombing Prevention (OBP) develops and delivers a diverse curriculum of training and awareness products to various government officials, law enforcement, security staff, critical infrastructure operators, and other partners. Course descriptions are at [https://www.dhs.gov/bombing-prevention-training](https://www.dhs.gov/bombing-prevention-training). Popular options include Surveillance Detection, Protective Measures Course, and IED Search Procedures, Bomb Threat Management, and others. Courses may be requested and coordinated with your Protective Security Advisor or State Training Officer.

**American Red Cross, Colorado Region:** The Red Cross provides many current and practical business and organizational preparedness courses. Depending on your location, options include Bleeding Control and Active Shooter Survival. [https://www.redcross.org/take-a-class/train-my-employees](https://www.redcross.org/take-a-class/train-my-employees)

---

**Suspicious Activity Reporting (SAR) Resources**

**The Nationwide SAR Initiative:** The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) is a collaborative effort led by the U.S. Department of Justice in partnership with DHS, FBI, and State, local, tribal, and territorial law enforcement partners. This initiative provides a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information. If you wish to report suspicious information that you believe relates to terrorism, or that may result in the prevention of terrorism, please submit that information via the Colorado Information Analysis Center (CIAC) link found at [http://dhsem.state.co.us/prevention-security/ciac](http://dhsem.state.co.us/prevention-security/ciac). Your report will be immediately forwarded to the FBI, DHS, and local law enforcement.

Local Law Enforcement  
Colorado Information Analysis Center (CIAC)  
911  
877-509-2422  
(imminent activity)  
(any suspicious activity)

---

**If You See Something, Say Something:** The nationwide "If You See Something, Say Something™" public awareness campaign is a simple and effective program to raise public awareness of indicators of terrorism and terrorism-related crime, and to emphasize the importance of reporting suspicious activity to the proper local law enforcement authorities. The campaign was originally used by New York’s Metropolitan Transportation Authority (MTA), which has licensed the use of the slogan to DHS for anti-terrorism and anti-terrorism crime related efforts. [http://www.dhs.gov/seesay](http://www.dhs.gov/seesay) contains materials, contact information for customizing materials, and videos.

**Safe2Tell:** Designed to help Colorado students anonymously report any threatening behavior that endangers them, their school, friends, family, or community. [http://safe2tell.org/](http://safe2tell.org/)

---

7  
Colorado Homeland Security Resource Guide