Colorado Homeland Security Resources

Homeland Security

Table of Contents

Partnership 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 – includes the Daily Open-Source Information Report and travel security information. http://www.dhs.gov . The link to the DHS Critical Infrastructure Protection page, including many of the Infrastructure Protection Programs, is http://www.dhs.gov/files/programs/critical.shtm

- **Protective Security Advisors (PSA):** The PSA Program's primary mission is to secure critical infrastructure. Working with regional directors, PSAs conduct cross-cutting information sharing and coordination activities in support of these mission areas: Plan, coordinate, and conduct security surveys and assessments; Plan and conduct outreach activities; Support National Special Security Events (NSSEs) and Special Event Activity Rating (SEAR) Level I and II events; Respond to incidents; Coordinate and support improvised explosive device awareness and risk mitigation training. http://www.dhs.gov/protective-security-advisors

- **Intelligence Officers (IO):** IOs are deployed by the DHS Office of Intelligence and Analysis (I&A) to apply their intelligence skills at a local level, in collaboration with state, local, tribal, territorial, and private sector partners and the DHS Intelligence Enterprise, to promote information sharing and assist the implementation and execution of the intelligence cycle. IOs serve two primary roles: 1) partner with fusion centers to facilitate achievement of the *Baseline Capabilities for State and Major Urban Area Fusion Centers* and 2) manage the intelligence cycle in their area of responsibility to include the sharing of threat-related information between SLTT partners and the federal government. The information and intelligence products shared by IOs provide the federal government with local context on emerging threats and inform the national threat picture. http://www.dhs.gov/publication/deployed-intelligence-officers-and-protective-security-advisors

- **Cyber Security Advisors (CSA):** The CSA program mission is to provide direct coordination, outreach, and regional support in order to protect cyber components essential to the sustainability, preparedness, and protection of the Nation's Critical Infrastructure (CI) and State, Local, Territorial, and Tribal (SLTT) governments. CSAs bolster the cyber security preparedness, risk mitigation, and incident response capabilities of these entities and bring them into closer alignment with the federal government. CSAs represent a front line approach and promote resilience of key cyber infrastructures throughout the U.S. and its territories.

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/

- **Colorado Information Analysis Center (CIAC):** The CIAC provides an integrated, multi-discipline information sharing network to collect, analyze, and disseminate information to stakeholders in order to protect the citizens and the critical infrastructure of Colorado. http://dhsem.state.co.us/prevention-security/ciac

- **Support Branch:**. http://www.dhsem.state.co.us/preparedness/preparedness

    - The **Critical Infrastructure Protection (CIP) and Cyber Security Section** provides leadership and support to Colorado communities by working with private industry, state, local, tribal, territorial and federal partners to protect critical infrastructure, systems and assets that are vital to Colorado. The section manages the State's involvement in multiple critical infrastructure related federal programs and integrates provisions of the National Infrastructure Protection Plan (NIPP)

into Colorado's State Homeland Security Strategy. The section also spearheads innovative ways to encourage owners and operators of critical infrastructure to share information and partner with the state to protect vital infrastructure. Products & Services: Cyber Vulnerability Assessments; Physical Vulnerability Assessments; Administration of Cyber Intelligence/Information Sharing Network; Infrastructure Prioritization Program; Development of best security practices for prevention, protection, and mitigation of all threats and hazards to infrastructure; Infrastructure Branch Director during State Emergency Operations Center activations; and Cyber Liaison Officer Program.

- The **Preparedness Program** provides leadership and support to Colorado communities through the curation, development and sharing of all-hazards preparedness information and resources in a whole of community approach that encompasses prevention, protection, response, recovery and mitigation. Products & Services: Community Awareness Program (CAP) Training; 8 Signs of Terrorism; READY Business Training; Modular Training; Are you Ready? Training; PRND Training; State of Colorado Emergency Response Guide; Colorado Emergency Preparedness Partnership (CEPP) bulletins; Preparedness Brochures; File of Life; PRND Plans (Strategy, CONOPS Equipment Guidelines); Community Emergency Response Team (CERT); Youth Preparedness; Community Conversations; Firewise and Ready, Set, Go!; Outreach participation at preparedness events; Community Preparedness Advisory Council (CPAC); Preventative Radiological Nuclear Detection Program (PRND); and Emergency Response Guide Working Group.

- The **Training and Exercise Program** seeks to facilitate the collaborative design of a strategic and aligned training program based on federal guidelines and recognized standards for homeland security, emergency management, public and behavioral health, medical, and other sectors involved in the effective and efficient delivery of response and recovery services. The program strives to be recognized as a standard of excellence. Products & Services: Emergency Management Training ; Homeland Security Training; Training and Exercise Workshops (TEPW); National Domestic Preparedness Consortium (NDPC); Exercise Planning and Implementation; HSEEP Program; Emergency Management Academy; Public Health Training coordinated with the Colorado Department of Public Health and Environment (CDPHE); Emergency Management Institute (EMI); CO.Train Registration Portal; Training Delivery & Facilitation; IMT Training and Exercise Needs; and Colorado Wildfire and Incident Management Academy (CWFIMA).

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

The Counterterrorism Education Learning Lab (CELL): The CELL is a non-profit and non-partisan institution dedicated to educating citizens about one of the most important issues of our time - terrorism. The CELL's mission is to empower individuals and organizations with the tools to become more informed, prepared, and involved within their own communities in order to help combat the threat of terrorism. Their exhibit, Anyone – Anytime – Anywhere: Understanding the Threat of Terrorism, is a dynamic, interactive experience with content developed by world-renowned experts, that provides visitors with an in-depth of the history of terrorism, the methods terrorists employ, and the extent to which terrorism impacts societies around the world. http://www.thecell.org/

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

Developing High Quality Emergency Operation Plans for Houses of Worship: The guide provided recommendations in the development of plans not only to respond to an emergency, but also outline how organizations can plan for preventing, protecting against, mitigating the impact of and recovering from these emergencies. The guide translates lessons learned from the Administration's work on national preparedness to the school, IHE, and house of worship contexts, ensuring that these critical assets are benefitting from recent advancements in the emergency planning field. The guide introduces houses of worship to a new approach to planning that includes walking through different emergency scenarios to create a course of action for each objective the team is trying to accomplish. The guide emphasizes that successful planning requires all stakeholders be engaged in the planning process from the start – including community partners such as local law enforcement, fire officials, EMS and emergency management staff. https://www.fema.gov/media-library/assets/documents/33007

Nonprofit Security Grant Program: The Nonprofit Security Grant Program provides funding support for hardening and other physical security enhancements to nonprofit organizations that are at high risk of terrorist attack and located within one of the specific Urban Area Security Initiative areas. The NSGP also serves to promote coordination and collaboration in emergency preparedness activities among public and private community representatives as well as state and local government agencies. https://www.fema.gov/nonprofit-security-grant-program

Standard Response Protocol: Courtesy of the "i love u guys" Foundation, the Standard Response Protocol (SRP) is based not on individual scenarios but on the response to any given situation. Like the Incident Command System (ICS), SRP demands a specific vocabulary but also allows for great flexibility. The premise is simple - there are four specific actions that can be performed during an incident. When communicating these, the action is labeled with a "Term of Art" and is then followed by a "Directive." Execution of the action is performed by active participants, including students, staff, teachers and first responders. http://www.iloveuguys.org/srp.html

How to Assess the Safety & Security of Your Place of Worship: This material was developed to: 1.) Give you the information, ideas and guidelines you need to conduct an effective assessment of your place of worship, as it relates to people, places, assets, processes and programs, as well as emergency planning and continuity planning; and 2.) Encourage a focused and balanced approach to safety and security planning. http://www.santarosa.fl.gov/coad/documents/SafetyinChurch.pdf

Security Concerns for Churches: The Role of Greeters and Ushers: Greeters and ushers can have a leadership role in safety, security and emergency planning related to many concerns in a place of worship. Their knowledge and experiences about church schedules, members and visitors and concerns or problems they have observed or handled, can make them invaluable contributors to the overall church security program. http://storage.cloversites.com/theriverconference/documents/The%20Greeter%20and%20Usher%20Role%20In%20Church%20Security.pdf

Netsmartz Worksop: NetSmartz Workshop is an interactive, educational program of the National Center for Missing & Exploited Children® (NCMEC) that provides age-appropriate resources to help teach children how to be safer on- and offline. The program is designed for children ages 5-17, parents and guardians, educators, and law enforcement. With resources such as videos, games, activity cards, and presentations, NetSmartz entertains while it educates. Our Goals: Educate children on how to recognize potential Internet risks; Engage children and adults in a two-way conversation about on- and offline risks; and Empower children to help prevent themselves from being exploited and to report victimization to a trusted adult. http://www.netsmartz.org/Parents

Business Continuity Planning Suite: This software was created for any business with the need to create, improve, or update its business continuity plan. The Suite is scalable for optimal use by organizations of any size and consists of a business continuity plan (BCP) training, automated BCP and disaster recovery plan (DRP) generators, and a self-directed exercise for testing an implemented BCP. Businesses can utilize this solution to maintain normal operations and provide resilience during a disruption. http://www.ready.gov/business-continuity-planning-suite

Community Emergency Response Teams: Welcome to the Community Emergency Response Team (CERT) webpage. Here you can find resources, training and information about the CERT Program. 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#

National Infrastructure Protection Plan (NIPP): Our Nation's well-being relies upon secure and resilient critical infrastructure—the assets, systems, and networks that underpin American society. The National Infrastructure Protection Plan (NIPP) -- NIPP 2013: *Partnering for Critical Infrastructure Security and Resilience* -- outlines how government and private sector participants in the critical infrastructure community work together to manage risks and achieve security and resilience outcomes.. http://www.dhs.gov/national-infrastructure-protection-plan

Sector Specific Plans (SSP): PPD-21 assigns a federal agency, known as a Sector-Specific Agency (SSA), to lead a collaborative process for critical infrastructure protection within each of the 16 critical infrastructure sectors. Each Sector-Specific Agency is responsible for developing and implementing a sector-specific plan (SSP), which details the application of the NIPP concepts to the unique characteristics and conditions of their sector. Some are For Official Use Only (FOUO) – contact the NIPP program office at NIPP@dhs.gov to acquire the FOUO SSPs.

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 DHS and other Federal, State, tribal, and local analysts use PCII to:

- Analyze and secure critical infrastructure and protected systems,
- Identify vulnerabilities and develop risk assessments, and
- Enhance recovery preparedness measures.

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 which are organized by state organizations; Federal organizations; or mission areas such as emergency management, law enforcement, critical sectors, and intelligence. Users can securely share within their communities or reach out to other communities as needed. HSIN provides secure, real-time collaboration tools, including a virtual meeting space, instant messaging, and document sharing. HSIN also allows partners to work together instantly, regardless of their location, to communicate, collaborate, and coordinate. To request access to HSIN, please submit the following (Name, Employer, Title, Business email, Brief written justification) to HSINCS@hq.dhs.gov. http://www.dhs.gov/hsin-cs

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 Sellers of "qualified anti-terrorism technologies." Our aim is to ensure the possessors of such anti-terrorism technologies are not deterred by the threat of liability from developing and commercializing products and technologies that could save lives in the event of a terrorist attack. As part of the Homeland Security Act of 2002, Public Law 107-296, Congress enacted several liability protections for providers of anti-terrorism technologies. The SAFETY Act provides incentives for the development and deployment of anti-terrorism technologies by creating a system of "risk management" and a system of "litigation management." The purpose of the Act is to ensure that the threat of liability does not deter potential manufacturers or Sellers of anti-terrorism technologies from developing and commercializing technologies that could save lives. The Act creates certain liability limitations for "claims arising out of, relating to, or resulting from an act of terrorism" where qualified anti-terrorism technologies have been deployed. https://www.safetyact.gov/pages/homepages/Home.do

TRIPwire Community Gateway: The TRIP*wire* Community Gateway is a Web portal designed specifically for critical infrastructure owners, operators, and private security personnel. The Gateway provides expert threat analyses, reports, and planning documents to help key private sector partners anticipate, identify, and prevent Improvised Explosive Device (IED) incidents. https://www.dhs.gov/tripwire

Multi-Jurisdiction IED Security Planning (MJIED): The Multi-Jurisdiction Improvised Explosive Device Security Planning (MJIEDSP) Program is a systematic process that fuses counter-IED capability analysis, training, and planning to enhance urban area IED prevention, protection, mitigation, and response capabilities. The MJIEDSP assists with collectively identifying roles, responsibilities, capability gaps and with optimizing limited resources within a multi-jurisdictional planning area. The DHS Office of Infrastructure Protection's Office for Bombing Prevention (OBP) works closely with communities to provide expertise on planning and operational requirements for IED incident preparedness in alignment with the National Preparedness Goal and its core capabilities. (Contact your PSA for further information)

National Counter-Improvised Explosive Device Capabilities Analysis Database (NCCAD): The National Counter-Improvised Explosive Device (IED) Capabilities Analysis Database (NCCAD) is an assessment program that uses a consistent and repeatable analytical methodology to assess and analyze the capabilities of bomb squads, explosive detection canine teams, dive teams, and Special Weapons and Tactics Teams throughout the United States. NCCAD assessments measure the capability elements of personnel, equipment, and training required for effective prevention, protection, and response to IED threats. This integrated information provides a snapshot of local, State, regional, and national counter-IED preparedness that informs decision makers on policy decisions, resource allocation for capability enhancement, and crisis management. (Contact your PSA for further information)

Private Sector Clearance Program (PSCP): The vast 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 – this may include your position as an owner/operator of a Critical Infrastructure entity, a subject matter expert, or other position which would necessitate the holding of a security clearance. (Contact your PSA for further information)

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

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/#

Colorado School Safety Resource Center (CSSRC): The mission of the Colorado School Safety Resource Center (CSSRC) is to collaboratively assist local schools and communities to create safe and positive school environments for Colorado students in all pre-K-12 and higher education schools. 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. The CSSRC supports schools and local agencies in their efforts to prevent, prepare for, respond to, and recover from all types of emergencies and crisis situations. www.Colorado.gov/CSSRC

Safe2Tell: Designed to help students anonymously report any threatening behavior that endangers them, their friends, family, or community. http://safe2tell.org/

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

CONNECT Colorado: While businesses and governments understand the value of planning for continuity of operations, too often the planning is done without a partnership between companies, industry sectors, or government. CONNECT Colorado is a voluntary registry of private sector business resources such as trucks, equipment, skilled personnel, and power that can be called upon by state and local emergency management organizations during disasters. http://thecepp.org/upgrade/?q=content/connect-colorado-overview

Ready Colorado: READYColorado.com is designed to help every Coloradan become prepared to respond to and recover from a wide array of disasters ... both natural and human-caused. www.readycolorado.com

Ready.gov: is 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. The goal of the campaign is to get the public involved and ultimately to increase the level of basic preparedness across the nation. www.ready.gov

Cyber Resources

U.S. Computer Emergency Readiness Team (CERT): The Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) leads efforts to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation while protecting the constitutional rights of Americans. US-CERT strives to be a trusted global leader in cybersecurity - collaborative, agile, and responsive in a dynamic and complex environment. https://www.us-cert.gov/

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT): ICS-CERT operates within the National Cybersecurity and Integration Center (NCCIC), a division of the Department of Homeland Security's Office of Cybersecurity and Communications (DHS CS&C). NCCIC/ICS-CERT is a key component of the DHS Strategy for Securing Control Systems. The primary goal of the Strategy is to build a long-term common vision where effective risk management of control systems security can be realized through successful coordination efforts. Report cyber related infrastructure incidents at ics-cert@hq.dhs.gov

Critical Infrastructure Cyber Community Voluntary Program (C³): As part of Executive Order (EO) 13636, the Department of Homeland Security (DHS) launched the Critical Infrastructure Cyber Community or C³ (pronounced "C Cubed") Voluntary Program to assist the enhancement of critical infrastructure cybersecurity and to encourage the adoption of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (the Framework), released in February 2014. The C³ Voluntary Program was created to help improve the resiliency of critical infrastructure's cybersecurity systems by supporting and promoting the use of the Framework. https://www.us-cert.gov/ccubedvp To contact us, please email us at ccubedvp@hq.dhs.gov.

Enhanced Cybersecurity Services (ECS): ECS is a voluntary information sharing program that assists critical infrastructure owners and operators as they improve the protection of their systems from unauthorized access, exploitation, or data exfiltration. DHS works with cybersecurity organizations from across the federal government to gain access to a broad range of sensitive and classified cyber threat information. DHS develops indicators based on this information and shares them with qualified Commercial Service Providers (CSPs), thus enabling them to better protect their customers who are critical infrastructure entities. ECS augments, but does not replace, an entities' existing cybersecurity capabilities. http://www.dhs.gov/enhanced-cybersecurity-services

Automated Information Sharing:

- **Trusted Automated eXchange of Indicator Information (TAXII):** The TAXII specification defines a set of services and message exchanges for sharing cyber threat information across organizational boundaries. While secure message exchange techniques do exist and are leveraged in various cybersecurity communities, TAXII aims to standardize how organizations and consortia can set up truly interoperable, automated sharing systems with each another. https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity

- **Structured Threat Information eXpression (STIX):** STIX is a language for communicating cyber threat information in a flexible, structured format suitable for automated interpretation to enable active defense and sophisticated analysis. STIX can express a highly extensive set of cyber threat characteristics, including detectable indicators of adversary activity (such as IP addresses and file hashes), attackers' tactical patterns (such as the "kill chain" phases), and target characteristics (such as version and patch level), and even courses of action that can be applied to remediate or protect potentially affected systems. 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, we gather and share information and intelligence with public and private sector partners worldwide. http://www.fbi.gov/about-us/investigate/cyber

USSS Electronic Crimes Task Forces (ECTF): The role of the U.S. Secret Service (USSS) has gradually evolved since the agency's 1865 inception, from its initial mandate — suppressing the counterfeiting of U.S. currency — to protecting the integrity of the nation's financial payment systems. During this time, as methods of payment have evolved, so has the scope of the Secret Service's mission. Computers and other chip devices are now the facilitators of criminal activity or the target of such, compelling the involvement of the Secret Service in combating cyber crime. The perpetrators involved in the exploitation of such technology range from traditional fraud artists to violent criminals - all of whom recognize new opportunities to expand and diversify their criminal portfolio. http://www.secretservice.gov/ectf_about.shtml

Physical Assessment Resources

Infrastructure Protection Gateway (IP Gateway): The IP Gateway is available to Federal, State, local, tribal, and territorial governments to enhance collaboration in support of your respective infrastructure protection mission activities and to provide a mechanism for more streamlined cross-government information sharing. Individuals within a State, locality, tribe, or territory interested in using the IP Gateway's tools and capabilities will be required to work through their respective IP Gateway administrator, who will serve as the primary point of contact for the IP Gateway and will be responsible for vetting and granting access to requesting homeland security professionals. To obtain access to the IP Gateway, all users must have a valid need to know, complete Protected Critical Infrastructure Information (PCII) Authorized User training, and complete all follow-on IP Gateway system training. The IP Gateway serves as the single interface through which DHS mission partners can access a large range of integrated IP tools, capabilities, and information to conduct comprehensive critical infrastructure vulnerability assessments, risk analysis, and event and incident planning. Highlights of the IP Gateway include the ability to access:

- A selection of physical and cyber vulnerability assessment and security survey capabilities
- Integrated data visualization and mapping capabilities to support complex data analysis
- An array of tools to support critical infrastructure planning and analysis, including a robust data search capability

http://www.dhs.gov/ipgateway

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. IST areas of focus include: facility overview and significance, barriers, building envelope, critical products, dependencies (natural gas, communications, electricity, IT, cyber, transportation, water, wastewater), entry control, illumination, information sharing, parking, physical security, protective measures, security force, security management, security systems, significant assets, and business continuity. 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.

Rapid Survey Tool (RST): The Rapid Survey Tool (RST) is a non-regulatory data collection capability that examines the most critical aspects of a facility's security and resilience posture with efficient, baseline questions. It is a shorter survey that allows assessors to gather the general status of a facility before deciding whether an in-depth survey is required. The Web-based Rapid Survey Tool, available through the Infrastructure Protection Gateway (IP Gateway), captures a facility's physical and operational security and resilience data. The data are then analyzed to determine the facility's relative security and resilience in comparison to the national average for similar facilities.

Infrastructure Visualization Platform (IVP): The IVP is a tactical 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 owners/ operators with a cross-platform tool that allows them to present data, make quick and informed decisions, and confidently respond to an incident. The information resulting from a IVP assessment is provided via an interactive IVP Report which incorporates the collected photos and video as well as the user-supplied data, including evacuation plans, standard operating procedures, geospatial and aerial facility views, schematic/floor plans, and vulnerability assessments.

Cyber Assessment Resources

Cyber Infrastructure Survey Tool (C-IST): The C-IST identifies and documents critical cyber security information including system-level configurations and functions, cyber security threats, cyber security measures, IT business continuity/disaster recovery and cyber security organizational management;

- Provide information to DHS, SSAs, and facility owner/operators to support cyber security planning and resource allocation
- Enhance overall capabilities, methodologies, and resources for identifying and mitigating gaps
- Facilitate cyber security information sharing
- Benchmark overall cyber security for all sectors and demonstrate how assets and sectors are reducing risk

Cyber Security Evaluation Tool (CSET): The Cyber Security Evaluation Tool (CSET®) is a Department of Homeland Security (DHS) product that assists organizations in protecting their key national cyber assets. It was developed under the direction of the DHS National Cyber Security Division (NCSD) by cybersecurity experts and with assistance from the National Institute of Standards and Technology. This tool provides users with a systematic and repeatable approach for assessing the security posture of their cyber systems and networks. It includes both high-level and detailed questions related to all industrial control and IT systems. http://www.ics-cert.us-cert.gov/Assessments

Cyber Resilience Review (CRR): The CRR is a one-day, no-cost, facilitated cyber security evaluation deployed across all 16 CIKR sectors as well as State, local, tribal, and territorial governments. It is based on the *CERT® Resilience Management Model (RMM)*, a process improvement model for managing operational resilience whose primary goal is to evaluate how CIKR providers manage cyber security of significant information services and assets (information, technology, facilities, and personnel). Its secondary goal is to identify opportunities for improvement in cyber security management and reduce operational risks related to cyber security. http://www.us-cert.gov/ccubedvp/self-service-crr

Cyber Resilience Workshop: Each workshop introduces stakeholders and practitioners to cyber resilience concepts and to capacity and capability building activities in key performance areas related to cyber security, IT operations, and business continuity. Workshop content and tutorial activities reinforce both operational risk management and emergency/crisis management activities for critical cyber infrastructure personnel. Participants will leave with tangible, useful “take-away” information related to risk-based decision-making and security planning for critical IT services. Participants will be engaged in structured activities, via drills and scenarios, and introduced to concepts through direct discussion. Built-in activities, supported by guidelines and templates help to examine capability building in operational resilience practices and go well beyond discussions centered exclusively on IT security controls and countermeasures.

Continuous Diagnostics & Mitigation Program: The CDM Program enables governments to expand their continuous monitoring capabilities by increasing their network sensor capacity, automating sensor collections, and prioritizing risk alerts. CDM offers commercial off-the-shelf (COTS) tools, with robust terms for technical modernization as threats change. First, agency-installed sensors perform an automated search for known cyber flaws. Results feed into a local dashboard that produces customized reports, alerting network managers to their worst and most critical cyber risks, based on standardized and weighted risk scores. Prioritized alerts enable agencies to efficiently allocate resources based on the severity of the risk. Progress reports track results, which can be shared among sister networks. Summary information can feed into an enterprise-level dashboard to inform and prioritize cyber risk assessments.

Online Training Resources

FEMA Emergency Management Institute (EMI): Through its courses and programs, EMI serves as the national focal point for the development and delivery of emergency management training to enhance the capabilities of federal, state, local, and tribal government officials, volunteer organizations, and the public and private sectors to minimize the impact of disasters on the American public. Click http://training.fema.gov/EMIWeb//IS/crslist.asp. This link takes you to a list of about 60 independent study courses – they take under 3 hours to complete and you receive a diploma from FEMA. 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)

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. Be alert for the eight signs of terrorism! http://www.youtube.com/watch?feature=player_embedded&v=iWnKvhVnl9U

Active Shooter, What Can You Do: The Department of Homeland Security (DHS) announces the availability of a new Independent Study Course titled: *Active Shooter, What You Can Do (IS-907),* a no-cost training course developed to provide the public with guidance on how to prepare for and respond to active shooter crisis situations. A certificate from FEMA EMI is awarded to participants who complete the course and pass a short final exam. This new online training is available through the Federal Emergency Management Agency (FEMA) Emergency Management Institute (EMI) at http://training.fema.gov/EMIWeb/IS/IS907.asp

Run. Hide. Fight. Surviving An Active Shooter Event Video: This video, produced by the Houston Mayor's Office of Public Safety and Homeland Security, dramatizes an active shooter incident in the workplace. Its purpose is to educate the public on how to respond during such an incident. Warning: The initial sequence in this video may be disturbing. https://www.fbi.gov/about-us/cirg/active-shooter-and-mass-casualty-incidents/run-hide-fight-video

Active Shooter Preparedness: The Department of Homeland Security (DHS) aims to enhance preparedness through a "whole community" approach by providing training, products, and resources to a broad range of stakeholders on issues such as active shooter awareness, incident response, and workplace violence. In many cases, there is no pattern or method to the selection of victims by an active shooter, and these situations are by their very nature are unpredictable and evolve quickly. 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

Cyber Training – Web-Based: ICS-CERT has web-based courses which focus on control systems and cyber-related threats which are aimed at the private sector. http://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT

- ICS-CERT Virtual Learning Portal

Onsite Training Resources

https://www.dhs.gov/bombing-prevention-training

Surveillance Detection Course for Law Enforcement & Security Professionals: This course, designed for municipal security officials, State and local law enforcement with jurisdictional authority over critical infrastructure facilities, and critical infrastructure operators and security staff of critical infrastructure facilities, provides participants with the skills and knowledge to establish surveillance detection operations to protect critical infrastructure during periods of elevated threat. Consisting of five lectures and two exercises, the course increases awareness of terrorist tactics, attack history, and illustrates the means and methods used to detect surveillance**.** (3-days, up to 25 participants)

Homeland Security

IED Counterterrorism Workshop: This awareness level workshop is designed to enhance the knowledge of Law Enforcement and Private Sector security professionals by providing exposure to key elements of the improvised explosive device (IED) threat, surveillance detection methods and soft target awareness. The workshop illustrates baseline awareness and prevention actions that reduce vulnerabilities to counter the threat along with collaborating information sharing resources to improve preparedness. This designed approach better enables the owners and operators of critical infrastructure and key resources to deter, prevent, detect, protect against, and respond to terrorist use of explosives in the United States. (Four sessions over 2 days or two, 8 hour sessions over 2 days; up to 250 participants per session)

Protective Measures Course: This course is designed to provide executive and employee level personnel in the public/private sector with the knowledge to identify the appropriate protective measures for their unique sector. The course focuses on providing information pertaining to available protective measures and strategies for selecting which protective measures are most appropriate. The course focuses on teaching the student the threat analysis process, terrorist methodology and planning cycle, available protective measures, and determining which protective measures to employ. (2 days, up to 35 participants)

Bomb Making Materials Awareness Program: The Bomb Making Materials Awareness Program (BMAP) is designed to increase private sector awareness of activities associated with bomb-making, including the manufacture of homemade explosives (HMEs). BMAP provides audience-appropriate awareness information on suspicious behavior, hazardous materials, precursor chemicals, and other bomb-making related information. It is communicated as part of DHS's TRIPwire and National IED Prevention and Awareness Campaign and was developed in cooperation with the FBI.

Improvised Explosive Device (IED) Awareness/ Bomb Threat Management Workshop: Enhances participants' knowledge, skills, and abilities concerning IEDs. Outlines specific safeties associated with bomb threat management and IED awareness, incidents, and prevention.

Improvised Explosive Device Search Procedures: Increases preparedness of security personnel and facility managers of sites that are hosting a special security event. Focuses on general safeties used for specialized search and explosives sweeps and can be tailored to meet specific participants' needs.

Vehicle Borne IED Detection Course: This course improves participant's ability to successfully inspect for, detect, identify components of and respond to a Vehicle Borne Improvised Explosive Device (VBIED). The target audience consists of first responders, public safety officers, and private security professionals tasked with inspecting vehicles for contraband, explosives, or any dangerous goods. The course covers the VBIED threat, explosives, IEDs, and vehicle inspections, enabling participants to deter, protect against, and respond to terrorist use of explosives in the United States.

Cyber Training – Instructor-Led: ICS-CERT has instructor-led courses which focus on control systems and cyber-related threats which are aimed at the private sector. http://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT

- Introduction to Control Systems CyberSecurity (101) – 1 day
- Intermediate Cybersecurity for Industrial Control Systems (201, lecture only) – 1 day
- Intermediate Cybersecurity for Industrial Control Systems (202, lab/exercises) – 1 day
- ICS Cybersecurity (301) – 5 days

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 (DOJ) in partnership with DHS, FBI, and State, local, tribal, and territorial law enforcement partners. This initiative provides law enforcement with another tool to help prevent terrorism and other related criminal activity by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information. Homeland Security is everyone's responsibility. 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. Your report

will be immediately forwarded to the FBI, DHS, and local law enforcement. We always recommend contacting law enforcement as the first step.

Local Law Enforcement	**911**	(imminent activity)
Colorado Information Analysis Center (CIAC)	720-852-6705	(any suspicious activity)
TSA General Aviation Hotline	866-GA-SECURE	(suspicious general aviation 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/if-you-see-something-say-something%E2%84%A2-campaign

Download an electronic copy of the “See Something, Say Something” campaign video. http://www.dhs.gov/xlibrary/videos/fema-tp.031011.zip. The video is 10-minutes in length. Click ‘Save’ to load this onto your hard drive (95MB zip file – becomes a .wmv file).

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/

Homeland Security