U.S. Department of Homeland Security

Summary of Resources for State, Local, Tribal, Territorial, and Campus Law Enforcement Partners

January 2024

Homeland Security

Dear Law Enforcement Partners:

Your service, sacrifice, and commitment to the safety and resilience of our communities, especially in the face of new and evolving threats, represent the very best of our great nation. The Department of Homeland Security is extraordinarily proud to support you and to serve alongside you.

We are committed to ensuring every law enforcement agency – regardless of size, funding, or resources – has the tools and support necessary to carry out the work that is essential to maintaining our security. This Law Enforcement Resource Guide highlights many of the Department's threat resilience resources available to you, including training and grant opportunities.

To learn more about the Law Enforcement Resource Guide and other DHS means of support for the law enforcement community, please contact the DHS Office for State and Local Law Enforcement at OSLLE@hq.dhs.gov.

Thank you for your continued collaboration, and for your service to our nation.

Sincerely,

Alejandro N. Mayorkas

Secretary of Homeland Security

Table of Contents

Preparedness and Prevention

U.S. Secret Service National Threat Assessment Center (NTAC)

The U.S. Secret Service National Threat Assessment Center (NTAC) provides research, guidance, case studies, training, and consultation on topics related to behavioral threat assessment and the prevention of targeted violence. NTAC's multidisciplinary team of subject matter experts is comprised of social science researchers and regional program managers who empower our partners in law enforcement, schools, government, and other public and private sector organizations to combat targeted violence impacting communities across the United States.

DHS Common Operating Picture (COP)

The DHS Common Operating Picture (COP) provides Homeland Security Enterprise professionals with enhanced situational awareness for incidents and events of national significance as defined by the National Operations Center (NOC). The solution provides strategic-level situational awareness that facilitates timely decision support prior to, during and in the aftermath of an incident or event of national significance. Incidents and events can cover any of the DHS mission areas to:

- Counter Terrorism and Homeland Security Threats,
- Secure U.S. Borders and Approaches,
- Secure Cyberspace and Critical Infrastructure,
- Preserve and Uphold the Nation's Prosperity and Economic Security,
- Strengthen Preparedness and Resilience, and;
- Champion the DHS Workforce and Strengthen the Department.

The DHS COP is available to all Homeland Security partners to include State, Local, Tribal, Territorial, and Campus (SLLTC) Law Enforcement, and is accessed through the Homeland Security Information Network (HSIN). Any individuals looking for access can send an email to: NOC.DHSCOP.Access@hq.dhs.gov

DHS Center for Prevention Programs and Partnerships (CP3)

The DHS Center for Prevention Programs and Partnerships (CP3) provides technical, financial, and educational assistance to empower local efforts to prevent targeted violence and terrorism. CP3 invests in the establishment, enhancement, and expansion of prevention projects through the Targeted Violence and Terrorism Prevention (TVTP) Grant Program. CP3 collaborates with communities across the country to establish and expand local prevention networks that reduce the risks of targeted violence and terrorism and convenes and educates communities on violence prevention solutions.

Resources for the Faith-Based Community

The DHS Center for Faith-Based and Neighborhood Partnerships works with partners across every level of government and in local communities to help faith and community leaders improve the safety and security of places of worship and community spaces. Further, DHS's Cybersecurity and Infrastructure Security Agency (CISA) provides several resources to help maintain the safety and security of houses of worship and related facilities, including assessments to identify key vulnerabilities. Learn more about resources for the faith-based community.

If You See Something, Say Something® Campaign

Informed and alert communities play a critical role in keeping our country safe. The DHS If You See Something, Say Something® campaign partners with state, local, tribal, and territorial governments, as well as private and nonprofit organizations, to raise public awareness about the importance of reporting suspicious activity to law enforcement to prevent acts of terrorism. The campaign offers free materials to help its partners promote the campaign.

Securing Public Gatherings

Public gatherings and crowded places are increasingly vulnerable to terrorist attacks and other extremist activity because of their relative accessibility and large number of potential targets.

To help organizations of all sizes mitigate potential risks in today's dynamic and rapidly evolving threat environment, CISA provides several resources related to securing soft targets like public gatherings and special events, Hometown Security program. including through its robust Physical Security resources portfolio.

National Threat Evaluation and Reporting (NTER) Office

The National Threat Evaluation and Reporting (NTER) Office works with state, local, tribal, territorial, and campus partners. NTER is a collaborative effort to share information and resources with public and private sector partners to assist in threat mitigation and targeted violence prevention by advancing partners' ability to identify, investigate, assess, report, and share tips and leads linked to emerging homeland security threats, while providing a host of information sharing services including program support, resources, and training. Review the Behavioral Approach to Violence Prevention Summary and all other NTER resources. Contact the NTER Office at NTER.MTP@hq.dhs.gov.

DHS Special Events Program (SEP)

The DHS Special Events Program (SEP) manages the National Special Event Data Call (NSEDC), which is an annual process that relies on the voluntary participation of states and territories to collect information on events occurring in their jurisdictions. Over 40,000 events are voluntarily submitted to the NSEDC by state and local authorities each year. The primary data collection period opens the first week of August and remains open for six weeks. The SEP continues to accept event submissions throughout the year as “short notice events.” All events submitted to the NSEDC receive a Special Events Assessment Rating (SEAR) that is applied using a risk-based analytical approach. Questions about SEAR or NSEDC can be directed to the DHS Special Events Program at: DHSSpecialEvents@hq.dhs.gov.

Active Shooter Preparedness

Active shooter incidents are often unpredictable and evolve quickly. During these incidents, being prepared can play an integral role in mitigating the impacts of a shooting. CISA aims to enhance preparedness through a "whole community" approach by providing products, tools, and resources to help you prepare for and respond to an active shooter incident. In addition, you can find the active shooter resources translated into other common languages on the Translated Active Shooter Resources webpage.

Conflict Prevention Techniques

CISA offers a variety of tools and resources to empower and educate employees, citizens, patrons, or any person with the skills and support they need to identify and report suspicious behavior. CISA recognizes the power that a single individual can have in deterring threats and preventing harm. CISA’s Conflict Prevention techniques are tailored to harness the power of the individual in securing the safety of our nation.

DHS Counter-IED Capabilities Assessment (CCA)

The Counter-IED Capabilities Assessment (CCA) helps communities understand their level of preparedness to counter complex attacks involving improvised explosive devices. Unit Level Assessments measure the readiness of individual units—such as bomb squads, dive teams, and explosive detection canine teams--in terms of their Personnel, Organization, Equipment, Training, and Exercises (POETE). Community Level Assessments take stock of the preparedness of entire jurisdictions to prevent, protect against, mitigate, respond to and recover from IED attacks.

Bombing Prevention

The CISA Office for Bombing Prevention (OBP) leads DHS’s efforts to enhance the nation’s ability to prevent, protect against, respond to, and mitigate the use of explosives against critical infrastructure, the private sector, and federal, state, local, tribal, territorial, and campus entities. OBP offers specialized resources for information sharing and decision support, improvised explosive device awareness training, capability analysis and planning for response to bomb threats and incidents, and coordination of national and intergovernmental bombing prevention efforts.

Equipment Assessment and Validation

The Science and Technology Directorate's (S&T) System Assessment and Validation for Emergency Responders (SAVER) program is managed by the National Urban Security Technology Laboratory and provides information on commercially available equipment to assist law enforcement with making informed purchasing decisions.

Known as "Consumer Reports for First Responders," SAVER reports on available technologies and how they perform under realistic conditions. SAVER has published law enforcement-related reports on augmented and virtual reality training systems, body cameras, body armor for women, indoor position and location tracking in three dimensions, handheld language translators, night vison devices, RFID evidence management, tactical eyewear, blue UAS, vehicle tracking technology, walk through screening for mass casualty threats, and wireless surveillance camera systems.

Interagency Security Committee Best Practices for Making a Business Case for Security

Increasingly complex security challenges and a dynamic threat environment necessitate the requirement for a strong and agile security planning, programming, and budgeting process. To that end, CISA's "Best Practices for Making a Case for Security" publications assist security professionals in constructing a decision-making process or rationale for proceeding with a security project or security program, completing a benefit-cost analysis (BCA) to support spending decisions, applying these concepts to the Interagency Security Committee (ISC) Risk Management Process, and measuring success.

Counter-WMD Equipment Information

The DHS Countering Weapons of Mass Destruction (CWMD) Office provides resources for law enforcement and first responders to learn about the capabilities of equipment and software for the counter-WMD mission space.

- CWMD's Data Mining, Analysis and Modeling Cell (DMAMC) brings together subject matter experts from the CWMD community with the processes and tools necessary to maintain and analyze test data. The data can then be used to respond to technical questions from the law enforcement community. To contact DMAMC, email DMAMC1@hq.dhs.gov.
- CWMD's Directed Testing Program conducts test campaigns using commercially available Chemical, Biological, Radiological, and Nuclear (CBRN) detection and identification systems to assist federal, state, local, tribal, territorial, and campus partners in developing operational concepts, procedures, and doctrine for CBRN detection. The CWMD Directed Testing Program hosts an Annual Outreach Symposium each June to collect information from the CBRN community on current needs that this program can address.

National Biosurveillance Integration Center

The National Biosurveillance Integration Center (NBIC) is located within Department of Homeland Security Countering Weapons of Mass Destruction Office as a unique national resource. NBIC collaborates with and serves as a bridge between federal and SLTTC agencies to integrate information from thousands of sources related to biological threats to human, animal, plant, and environmental health to improve early warning and situational awareness. NBIC reports and products enable government agencies at all levels to make more informed decisions at the tactical, operational, and strategic levels. For more information on NBIC SLTTC engagements and SLTTC access to NBIC products, email CWMD.NBIC@hq.dhs.gov.

Information and Intelligence Sharing

DHS Office of Intelligence and Analysis (I&A)

Intelligence and Analysis (I&A) is the only member of the Intelligence Community statutorily charged with bi-directional information and intelligence sharing with SLTTC and private sector partners. DHS is committed to sharing actionable and timely information and intelligence with these partners at the lowest classification level possible. Learn more about state and local engagement.

I&A has over 130 Intelligence Officers (IOs) assigned at fusion centers and other strategic locations to proactively engage and share threat information with federal, SLTTC, and other related agencies and the private sector to protect critical infrastructure and local communities. These IOs are available to share threat intelligence with organizations that have historically been targeted for violence. I&A IOs frequently partner with fusion centers and other state and local officials, CISA, and the Federal Bureau of Investigation (FBI) to analyze threats, gather and report threat information to DHS and the Intelligence Community, and to provide intelligence support during planning and execution of National Special Security Events (NSSEs) and other large-scale special events. Learn more about other intelligence elements.

DHS National Operations Center (NOC)

The National Operations Center (NOC) is a 24/7 federal operations center which serves as the primary, national-level hub for situational awareness, a common operating picture, information fusion, information sharing, and executive communications per the Homeland Security Act of 2002. It provides timely reporting and products derived from media, DHS Components, federal, state, local, tribal, and territorial governments, and private sector reporting. Federal, state, and local law enforcement officers from select locations across the country are integrated into NOC daily operations. The NOC can be reached at 202-282-8101.

Homeland Security Information Network (HSIN)

DHS manages the Homeland Security Information Network (HSIN) platform, which is DHS's official system for the trusted sharing of Sensitive but Unclassified information between federal, SLTTC, international, and private sector partners. These partners use HSIN to access products and data, securely send requests, coordinate operations, respond to incidents, and share information to help keep communities safe. Within HSIN, there are dozens of communities of interest that provide valuable resources to law enforcement, including:

- HSIN - Intelligence (HSIN-Intel), which provides federal and SLTTC partners with a secure platform to share intelligence and information as well as conduct analytic exchanges. DHS launched the INTEL App in April 2022, which enables HSIN-Intel users to securely access and view intelligence products, receive breaking alerts, and search key topics related to homeland security via mobile devices.
- HSIN - Critical Infrastructure (HSIN-CI), which provides federal and SLTTC partners, critical infrastructure owners, and operators partners with a secure platform to share intelligence and information related to critical infrastructure protection.
- HSIN - Law Enforcement (HSIN-LE), which provides law enforcement officials at every level of government with means to collaborate securely with partners across geographic and jurisdictional boundaries.
- HSIN - Emergency Services (HSIN-ES), which provides federal and SLTTC emergency services sector partners tools to respond, prevent, protect, and recover from disasters, and the ability to collaborate with For Official Use Only (FOUO) and Law Enforcement Sensitive (LES) information.

Homeland Secure Data Network (HSDN)

DHS manages the Homeland Secure Data Network (HSDN), which is DHS's official system for the trusted sharing of *Secret-level information* between appropriately cleared federal and SLTTC partners. These partners use HSDN to access intelligence information, products, and data, and to share information to help keep communities safe. DHS deploys HSDN systems to fusion centers to provide a fixed location that serves as a hub for information sharing. DHS I&A IOs can assist in gaining access to these locations for cleared non-fusion center personnel. Learn more about the Office of Intelligence and Analysis.

Emergency Services Sector Risk Management Agency (ES SRMA)

CISA is the Sector Risk Management Agency (SRMA) for the Emergency Services Sector (ESS) and provides specialized sector-specific expertise to the ESS and supports programs and associated activities. The ES SRMA provides a variety of resources to support ESS security and resilience.

Multi-State Information Sharing and Analysis Center (MS-ISAC)

CISA also funds the Multi-State Information Sharing and Analysis Center (MS-ISAC) that is free for SLTTC agencies to join. CISA encourages SLTTC agencies to sign up to receive their free services and capabilities, as well as receive time sensitive alerts and information.

DHS Geospatial Information Infrastructure (GII)

DHS hosts the Geospatial Information Infrastructure (GII), a shared Sensitive But Unclassified (SBU) platform for users to access mission-essential geospatial data, map services, and geospatial applications. The GII provides analysis, visualization, and collaboration capabilities supplemented by comprehensive geospatial training, tradecraft, and support services.

Fusion Centers

State and major urban area fusion centers are owned and operated by state and local entities, and serve as primary focal points for the receipt, analysis, gathering, and sharing of threat-related information among federal, SLTTC, and campus partners. Fusion centers are uniquely situated to empower law enforcement and other front-line personnel to lawfully gather and share threat-related information, including through the Nationwide Suspicious Activity Reporting Initiative. Learn more about fusion centers.

DHS National Terrorism Advisory System (NTAS) Advisories

Through the National Terrorism Advisory System (NTAS), DHS provides the public with information regarding the threat landscape facing the United States and resources for how to stay safe. These efforts are in alignment with DHS's commitment to sharing actionable and timely information and intelligence with the broadest audience possible. Read the latest NTAS bulletin and learn more about the National Terrorism Advisory System.

Moving forward, the annual Homeland Threat Assessment will serve as the primary regular mechanism for articulating and describing the prevailing terrorism threat level, which has previously been done through our issuance of biannual NTAS bulletins.

In the future, the issuance of NTAS bulletins will be reserved for situations where we need to alert the public about a specific or imminent terrorist threat or about a change in the terrorism threat level.

DHS Technical Resource for Incident Prevention (TRIPwire)

Technical Resource for Incident Prevention (TRIPwire) is DHS's online, secure information-sharing and resource portal for bomb squads, emergency responders, military personnel, government officials, intelligence analysts, private sector security professionals, and critical infrastructure owners and operators. TRIPwire increases awareness of evolving extremist IED tactics, techniques, and procedures, by providing expert analysis and threat information gathered from open-source intelligence, extremist groups, and raw incident data collection and is available at no cost.

U.S. Secret Service Protective Intelligence eXchange (PIX)

The Protective Intelligence eXchange (PIX) facilitates information sharing among U.S. law enforcement agencies with a protective intelligence function to support behavior-based threat assessment. Users must have an active LEEP or RISSNet account. There is no cost. Agencies requesting PIX access must apply directly to the U.S. Secret Service.

Cybersecurity

Cybersecurity Best Practices

CISA's Cyber Essentials campaign helps local government agencies, law enforcement, and other organizations mitigate cybersecurity risk and increase resilience. Through the Federal Virtual Training Environment (FedVTE), law enforcement partners can access free online cybersecurity training. CISA also provides professional, no-cost assessments upon request and on a voluntary basis to help any organization mitigate risk and prevent malicious cyber activity. Learn more about cybersecurity best practices and sign up for cybersecurity alerts.

Shared Cybersecurity Services (SCS)

CISA's Shared Cybersecurity Services (SCS) is a portfolio of Cybersecurity and Infrastructure Security Agency (CISA)-funded contracts that provides federal civilian agencies, state fusion centers, and select information sharing and analysis centers with no-cost access to commercial Cyber Threat Intelligence (CTI) and services. SCS allows users to access, research, and enrich CTI through a commercial enterprise license. Core offerings include access to CTI management platforms, automated sharing, training and IT Support, and limited analytical support (e.g., Requests for Information [RFIs]). To request vendor accounts or receive detailed information on individual vendor services, please contact: CISA.CTIS.SCS_Info@cisa.dhs.gov.

Combatting Ransomware

Ransomware actors often paralyze systems and threaten to sell or leak exfiltrated data if the ransom is not paid. Ransomware attacks have become increasingly prevalent among SLTT government entities. DHS launched StopRansomware.gov, alongside the Department of Justice and other federal partners, as a one-stop website that pools together federal resources to help prevent and respond to this evolving threat. Learn more about combatting ransomware.

"*Shields Up*": Prepare, Respond, and Mitigate the Impact of Cyberattacks

CISA stands ready to help organizations prepare for, respond to, and mitigate the impact of cyberattacks. When cyber incidents are reported quickly, CISA can use this information to render assistance and help prevent other organizations from falling victim to a similar attack. CISA will also report incidents to law enforcement for investigative actions. CISA recommends all organizations – regardless of their size – adopt a heightened posture when it comes to cybersecurity and protecting their most critical assets. Through its Shields Up campaign, a cybersecurity awareness program for government and private sector stakeholders, CISA has compiled a catalogue of related free services and resources. Organizations can also report anomalous cyber activity and/or cyber incidents 24/7 to report@cisa.gov or (888) 282-0870. Learn more about "Shields Up."

U.S. Secret Service Cyber Fraud Task Forces

The U.S. Secret Service operates over 40 field office based Cyber Fraud Task Forces (CFTFs), with a mission to prevent, detect, mitigate complex cyber-enabled financial crimes, with the ultimate goal of arresting and convicting the perpetrators. Through a partnership with private industry, federal, SLTTC, and foreign law enforcement agencies, federal and state prosecutors, and academia, the CFTFs effectively leverage the collective expertise of a range of key stakeholders to combat cybercrime. The CFTFs are staffed with special agents, technical experts, investigative and forensic analysts, and SLTTC task force officers trained at the Secret Service's National Computer Forensic Institute (NCFI). The Secret Service CFTFs are supported by the Washington, D.C. based Criminal Investigative Division (CID) and its Global Investigative Operations Center (GIOC).

Cybersecurity and Physical Security Convergence

The Cybersecurity and Physical Security Convergence Guide is an informational guide about convergence and the benefits of a holistic security strategy that aligns cybersecurity and physical security functions with organizational priorities and business objectives. Cyber and physical assets represent a significant amount of security risk—each can be targeted, separately or simultaneously, to result in compromised systems and/or infrastructure. When physical security and cybersecurity divisions operate in silos, they lack a holistic view of security threats targeting their enterprise.

Sector Spotlight: Cyber-Physical Security Considerations for the Electricity Sub-Sector

The Sector Spotlight: Cyber-Physical Security Considerations for the Electricity Subsector is a CISA and Department of Energy (DOE) co-branded product that provides small and mid-sized municipalities, utility owner operators, and the broader critical infrastructure community with a quick-hit product that highlights key cyber-physical attack vectors facing the electricity sub-sector, best practices for mitigating risk, and recommendations for maintaining resilience.

Stadium Spotlight: Connected Devices and Integrated Security Considerations

The Stadium Spotlight: Connected Devices and Integrated Security Considerations is a CISA and National Center for Spectator Sports Safety and Security (NCS) co-branded product that provides stadium owner operators and security professionals with a snapshot of the connected stadium environment, key vulnerabilities and consequences, and recommended enterprise- and asset-level risk mitigations.

Autonomous Vehicle Security

Autonomous vehicles (AV) are connected cyber-physical systems designed to improve the movement of people and goods across the country. To understand and address the threats to AVs, CISA developed the Autonomous Ground Vehicle Security Guide: Transportation Systems Sector to provide organizations with information to enhance awareness of current systems, a new taxonomy to characterize cyber-physical threats related to AVs, and recommended strategies to mitigate security risks at both the enterprise and asset levels.

Cybersecurity Best Practices for Operating Commercial Unmanned Aircraft Systems (UAS)

Critical infrastructure operators, law enforcement, and all levels of government are increasingly incorporating Unmanned Aircraft Systems (UAS) into their operational functions. The Cybersecurity Best Practices for Operating Commercial Unmanned Aircraft Systems Guide provides best practices to help operators protect their networks, information, and personnel. Additionally, Secure Your Drone: Privacy and Data Protection Guidance provides security guidance for UAS owners and operators to protect their data and minimize privacy risks before, during, and after flights.

U.S. Immigration and Customs Enforcement Homeland Security Investigations Cyber Crimes Center (ICE HSI C3)

U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Cyber Crimes Center (C3) delivers computer-based technical services to support domestic and international investigations into cross-border crime. This state-of-the-art center offers support and training to law enforcement agencies to tackle cybercrime and operates a fully equipped computer forensics laboratory that specializes in digital evidence recovery and offers training in computer investigative and forensic skills.

Computer Forensic Unit

The Computer Forensics Unit supports local, state, and federal partners with advanced technical solutions, digital forensic training, and equipment for HSI Task Force Officers and subject matter expertise. To submit a request for assistance, agencies should contact their local HSI office.

Cyber Crimes Unit

A top priority for HSI is to improve collective law enforcement capabilities by providing training to partner law enforcement agencies. In response to initiatives to reduce opioid demand in the United States, the HSI C3 developed a cyber-training curriculum with a focus on dark web investigations and illicit payment networks, associated with opioid smuggling and distribution. This training has been successful in improving collective law enforcement capabilities against online marketplaces and tools for illicit trafficking. Additionally, HSI C3 provides network intrusion investigation training that addresses the concepts and investigative points associated with these investigations. Since 2017, HSI has delivered this training course in over 70 locations worldwide to more than 12,000 state, local, federal, and international law enforcement personnel.

Child Exploitation Investigations Unit (CEIU)

The HSI CEIU uses cutting-edge technologies combined with traditional investigative techniques to identify and rescue child victims of sexual exploitation throughout the world, investigate producers and distributors of child sexual abuse material (CSAM), and target individuals who travel abroad for the purpose of engaging in sex with minors, also known as Transnational Child Sex Offenders (TCSO). The CEIU trains HSI personnel and state, local, federal, and international law enforcement partners in child exploitation investigations. HSI also offers Project iGuardian, an outreach effort to communicate the dangers of web-based environments, how to help kids stay safe online, and how to report abuse and suspicious activity. Agencies should request assistance in child exploitation cases by sending an email to ceiu_intake@ice.dhs.gov.

Critical Infrastructure Protection

Critical Infrastructure Vulnerability Assessments

CISA's Integrated Operations Division (IOD) conducts voluntary specialized field assessments to identify vulnerabilities, interdependencies, capabilities, and cascading effects of impacts on U.S. critical infrastructure. Learn more about the CISA services catalog.

CISA Regions

Across the nation, CISA offers a range of cyber and physical services to support the security and resilience of critical infrastructure owners and operators and state, local, tribal, territorial, and campus partners. Our experts collaborate with critical infrastructure partners and communities at the regional, state, county, tribal, and local levels. CISA's Regions proactively engage with federal, state, local, tribal, territorial, and campus partners and the private sector to protect critical infrastructure. The CISA Security Advisors are subject matter experts and are trained to identify vulnerabilities and mitigate risk and are available to advise and assist organizations that have historically been targeted for violence. The Regions frequently partner with other Federal Department and Agencies such as the FBI and U.S. Secret Service to provide vulnerability assessments, security planning, and coordination during National Special Security Events and other large-scale special events.

Critical Infrastructure Exercises

CISA conducts physical and cyber security exercises with government and industry partners to enhance the security and resilience of critical infrastructure. These exercises provide effective and practical mechanisms to identify best practices, lessons learned, and areas for improvement in plans and procedures.

Unmanned Aircraft Systems (UAS) – Critical Infrastructure

In addition to recreational use, unmanned aircraft systems (UAS)—also known as unmanned aerial vehicles (UAV) or drones—are used across our nation to support firefighting and search and rescue operations, to monitor and assess critical infrastructure, to provide disaster relief by transporting emergency medical supplies to remote locations, and to aid efforts to secure our borders. However, UAS can also be used for malicious schemes by terrorists, criminal organizations (including transnational organizations), and lone actors with specific objectives. Learn more about unmanned aircraft systems and critical infrastructure.

ChemLock

CISA's ChemLock program provides no-cost voluntary services and tools to help facilities that possess dangerous chemicals better understand the risks they face and improve their chemical security posture in a way that works for their business model. These services and tools include chemical security guidance documents, fact sheets, and flyers, as well as training, on-site security assessments and assistance, and exercises/drills with new products and services being added regularly. As part of the ChemLock program, CISA encourages facilities with dangerous chemicals to contact and work with local law enforcement and first responders to build collaborative relationships so that the first time that first responders are at the site is not the day of an incident.

Doxing and Critical Infrastructure

Doxing refers to the internet-based practice of gathering an individual's personally identifiable information (PII)— or an organization's sensitive information—from open source or compromised material—and publishing it online for malicious purposes. Critical infrastructure organizations maintain digital databases of PII and organizationally sensitive information, making them ripe targets for doxing attacks. CISA created the Mitigating the Impacts of Doxing on Critical Infrastructure resource which provides information on protective and preventative options for individuals and organizations, doxing case studies, and mitigation options should a doxing incident occur. Learn more about doxing and critical infrastructure.

Joint Cyber Defense Collaborative (JCDC)

In our globally interconnected world, our critical infrastructure and way of life face a wide array of serious risks with significant real-world consequences. CISA established Joint Cyber Defense Collaborative (JCDC) to unify cyber defenders from organizations worldwide and to enable co-equal partnership between government and the private sector. JCDC seeks to enable true co-equal partnership between government and the private sector.This diverse team proactively gathers, analyzes, and shares actionable cyber risk information to enable synchronized, holistic cybersecurity planning, cyber defense, and response.

Insider Threat Mitigation

Insider threat incidents are possible in any sector or organization. To combat insider threats, organizations can implement a proactive, prevention-focused mitigation program to detect and identify threats, assess risks, and manage those risks before an incident occurs.

Homeland Infrastructure Foundation-Level Data (HIFLD)

The DHS Geospatial Management Office provides access to FOUO and licensed critical infrastructure geospatial data through the Homeland Infrastructure Foundation-Level Data (HIFLD) portal. HIFLD delivers current and authoritative mission critical geospatial data of the highest possible quality to meet the emerging and enduring needs of stakeholders and consumers throughout the Homeland Security Enterprise.

Achieving Integrated Security: An Interagency Security Committee Best Practice

The Achieving Integrated Security document seeks to create a paradigm shift by promoting the integration of organizational security disciplines to converge IT and security functions and provides:

- Guidance to assist federal executive branch departments and agencies in achieving integrated security through best practices and methodologies.
- Recommendations for planning, promoting, and implementing a unified effort between several related areas; including information security, physical security, cybersecurity, and information technology.
- A planning model for merging of parallel risk management processes, optimization of organizational alignment, recommended training, and performance management.

Technology Training Events – Critical Infrastructure (TTE-CI)

CISA TTE-CIs are conducted in collaboration with the United States Bomb Technician Association, the Federal Bureau of Investigation (FBI) Critical Incident Response Group and the FBI Hazardous Devices School. These events bring Public Safety Bomb Squads together with industry and owner/operators of critical infrastructure to identify novel means of safely rendering explosive devices safe without creating second order impacts to the surrounding critical infrastructure.

School Safety and Security

School Safety and Security Resources

CISA's K-12 School Security Guide (3rd Edition) and School Security Assessment Tool (SSAT) demonstrate how a layered, systems-based approach to school physical security planning can help schools create safe and secure learning environments. The K-12 School Security Guide (3rd Edition) provides a comprehensive doctrine and systems-based methodology for vulnerability assessment, planning, and implementation of layered physical security elements. The SSAT incorporates a school's specific context and applies the systems-based approach described in the guide to improve a school's physical security by focusing on some of the most common incidents of crime and violence that K-12 schools in the United States face today. Three companion products are available to assist audiences with the SSAT: a User Guide, a Technical Appendix, and a How-To-Video.

CISA and the U.S. Secret Service's (USSS) K-12 Bystander Reporting Toolkit supports K-12 schools and districts in strengthening school safety reporting programs and encouraging bystander reporting among students and other members of the school community. The toolkit offers simple strategies and guidance to implement or enhance safety reporting programs and create a school environment where students are more willing and able to report concerns for the wellness and safety of themselves or others. This resource represents the latest effort in CISA's and USSS's shared school safety mission: providing schools with actionable, practical, and cost-efficient evidence-based practices toward preventing harm or acts of violence among our most important populations. Learn more about school safety.

SchoolSafety.gov

SchoolSafety.gov was created by DHS and the Departments of Education, Justice, and Health and Human Services to provide K-12 schools and districts with resources to help prevent, protect, mitigate, respond to, and recover from emergency situations.

National Training and Education Division (NTED)

FEMA's National Training and Education Division (NTED) provides several school safety-related courses, including for law enforcement in rural communities to respond to school-based emergencies.

U.S. Secret Service National Threat Assessment Center (NTAC)

The National Threat Assessment Center (NTAC) provides research and guidance to empower K-12 school personnel and other public safety professionals in preventing targeted school violence. NTAC created an operational guide with actionable steps to develop comprehensive targeted violence prevention plans for conducting behavioral threat assessments in schools. NTAC's research has examined 67 averted attack plots in K-12 schools from 2006-2018, as well as 41 completed K-12 attacks from 2008-2017.

Human Trafficking: Forced Labor and Sex Trafficking

DHS Center for Countering Human Trafficking

The DHS Center for Countering Human Trafficking (CCHT) drives criminal investigations of forced labor and sex trafficking through coordinated intelligence and evidence-based strategies; seeks improvements to delivery of victim protections, including victim-based immigration benefits, a national Continued Presence program for law enforcement, and robust identification; increases human trafficking victim identification through training, nationwide public awareness (through the Blue Campaign), and screening tools; incorporates proven and promising victim-centered practices into DHS policies and protocols; strengthens trade enforcement against the importation of goods produced with forced labor; and assists procurement implementation and enforcement efforts to prevent and deter human trafficking in DHS acquisitions and contracts.

Blue Campaign

The Blue Campaign is a national public awareness campaign designed to educate the public, law enforcement, and other industry partners to recognize the indicators of human trafficking and appropriately report possible cases. The Blue Campaign provides free awareness material and training to help prevent the vulnerable community, to deter buyers, and to protect those being victimized by human trafficking. Their awareness materials range from faith-based, school resource officers, campus police to a wide range of other audiences throughout the country.

The Blue Campaign develops awareness trainings and educational resources, including the Blue Campaign Campus Law Enforcement Guide, Campus Law Enforcement Pocket Card, and Campus Law Enforcement Training. These tools enable law enforcement and public safety officials to recognize and respond to suspected human trafficking cases in a campus environment using a victim-centered approach. Learn more about Blue Campaign.

Continued Presence Program

Through the Center for Countering Human Trafficking, DHS processes all Continued Presence (CP) applications for law enforcement nationwide. CP is a temporary immigration designation provided to individuals identified by law enforcement as trafficking victims who may be potential witnesses. CP is a renewable, two-year authorization that allows victims to remain in the United States, obtain a free work permit, and receive other federal benefits and services. In the earliest stages of an investigation, CP is the best vehicle for federal, SLTT, and campus law enforcement to obtain temporary and quick legal immigration protection for trafficking victims and may serve as a bridge to additional immigration protections for trafficking victims, including T nonimmigrant status. This combination of protections stabilizes victims, restores self-sufficiency, and improves their ability to assist law enforcement. To learn more about CP, please see the Continued Presence Resource Guide for submitting law enforcement agencies and civil attorneys which also provide instructions on how to request CP.

T Visas for Victims of Human Trafficking and U Visas for Victims of Qualifying Criminal Activities

T nonimmigrant status (also known as a "T visa") allows victims of human trafficking to remain in the United States on a temporary basis if they have complied with any reasonable request for assistance from law enforcement in the detection, investigation, or prosecution of human trafficking, and meet other eligibility requirements. U nonimmigrant status (also known as a "U visa") is for victims of certain qualifying crimes who have suffered substantial mental or physical abuse, have been, are being, or are likely to be helpful to law enforcement or government officials in the detection, investigation, or prosecution of the qualifying criminal activity, and meet other eligibility requirements. U.S. Citizenship and Immigration Services (USCIS) adjudicates these benefits and has developed resources for federal, state, local, tribal, territorial, and campus law enforcement, judges, family protective services, and other certifying agencies. These materials provide an overview of these legal immigration protections, share best practices for the certification process, include a list of additional resources for certifying agencies, and provide answers to frequently asked questions. Learn more about T Visa law enforcement.

USCIS provides training to certifying agencies and requests for training can be sent to T_U_VAWA Training@uscis.dhs.gov. USCIS also provides technical assistance to certifying officials and agencies who have inquiries about the T and U visa process. **Certifying officials can contact the T and U Visa Hotline for Certifying Agency inquiries at 240-721-3333.** ***This hotline is for certifying agencies only.***

"Concern" Law Enforcement Victim-Centered Approach Virtual Training

The Blue Campaign offers a virtual training for state and local law enforcement called "Concern." "Concern" is an asynchronous training simulation to encourage law enforcement personnel to use the victim- centered approach to combat human trafficking. The theme is protection through empathetic and non- judgmental interactions to establish rapport and show concern. This eLearning course, housed within e-FLETC, provides law enforcement and those likely to encounter victims practice opportunities for interviewing with a victim-centered approach. After completing this course, students will be able to 1) Advocate for the victim 2) Develop rapport and establish trust, and 3) Interview victims without judgement.

Human Trafficking Awareness Training

The Federal Law Enforcement Training Centers (FLETC) one-day Human Trafficking Awareness Training Program (HTAT) provides students an in-depth understanding of current indicators that law enforcement and the private sector may observe in industries known for human trafficking. An overview of federal statutes and applicable state law related to trafficking is referenced. The training is classroom oriented with case studies, videos, and student-centered learning activities to enhance the learning experience.

Human Trafficking Response Guide for School Resource Officers

The Blue Campaign recently created a Human Trafficking Response Guide for School Resource Officers. This toolkit provides information to school resource officers so they can recognize and report suspected incidents of human trafficking. Learn more about Blue Campaign Toolkits.

U.S. Secret Service Programs to Combat Crimes Against Children

The U.S. Secret Service, in collaboration with the National Center for Missing and Exploited Children (NCMEC), provides educational presentations to children (K-12) and adults through the Childhood Smart Program (CSP). These age-appropriate presentations help combat human trafficking and child exploitation by educating individuals on a wide range of topics. This valuable partnership between NCMEC and the Secret Service results in Secret Service personnel specially trained by NCMEC, spreading awareness and prevention through presentations to communities. In FY22, the Secret Service provided over 300 CSP presentations, reaching approximately 20,000 individuals. To request a CSP presentation, contact a local Secret Service field office or email fsdncmec@usss.dhs.gov.

U.S. Secret Service field offices participate in the Internet Crimes Against Children Task Force Program (ICAC program), sponsored by the U.S. Department of Justice Office of Juvenile Justice and Delinquency Prevention, which helps SLTTC law enforcement agencies develop an effective response to technology-facilitated child sexual exploitation and Internet crimes against children. Secret Service personnel work with their SLTTC partners, and state and federal prosecutors to investigate Internet crimes against children stemming from leads received through NCMEC's CyberTipline and from Internet service providers (ISPs).

U.S. Secret Service Forensic Resources to Support Investigations

The U.S. Secret Service combats crimes against children by supporting NCMEC and SLTTC law enforcement agencies with various types of forensic support. Secret Service forensic capabilities include polygraph examinations, video and audio enhancement, digital forensics speaker identification, questioned documents, latent prints, composite sketches, and geospatial information systems. To request forensic support, contact a local Secret Service field office. Learn more about Secret Service Field Office contacts.

Forced Labor in the Supply Chain

U.S. Customs and Border Protection (CBP) implements Section 307 of the Tariff Act of 1930, as amended (19 U.S.C. 1307) through the issuance of Withhold Release Orders and findings to prevent merchandise produced in whole or in part in a foreign country using forced labor from being imported into the United States. CBP also refers certain cases related to forced labor to other federal agencies for criminal prosecution. CBP is responsible for preventing the entry of products made with forced labor into the U.S market by investigating and acting upon allegations of forced labor in supply chains.

Research and Development

DHS Science and Technology Directorate (S&T)

S&T conducts evidence-based research to better understand the evolving threat landscape and works closely with first responders to improve their safety and effectiveness. S&T works directly with the national first responder community to increase responder's ability to address the challenging and evolving incidents they face when serving in our local communities. S&T works to quickly improve responder safety and effectiveness by utilizing the rapid prototyping of solutions, direct operational feedback, and rapid transition of solutions to the work force. S&T provides knowledge products on tactics & techniques and develops new equipment and technologies designed to improve responder protection, detection, mitigation, and awareness while responding to local emergencies. S&T provides knowledge products to enhance chemical awareness and personal protection, including less lethal (riot control) agents law enforcement may encounter. To accomplish this, S&T leverages Federally Funded Research and Development Centers, universities, industry, national laboratories, and in-house subject matter experts in fields such as Biological and Chemical Hazard and Threat Characterization, Countering Weapons of Mass Destruction, and Cybersecurity as well as emerging threats such as Counter Unmanned Aircraft Systems.

Public Safety and Violence Prevention (PSVP)

S&T conducts social science research to (a) support our understanding of individual motives for engaging in, and disengaging from, violent extremism; (b) develop and assist locally tailored interventions with local partners; and (c) evaluate the effectiveness of terrorism prevention activities and policies. PSVP focuses on targeted violence and terrorism prevention, human trafficking, and soft target security. This project aims to conduct social, behavioral, and economic science research to meet policy, operational, and public needs to improve the effectiveness of public safety and violence prevention efforts implemented by Federal, state, local, tribal, territorial and campus partners through evaluation research, capability development and enhancement, and data development. PSVP leverages inter/intra-agency, centers of excellence and international bilateral/multilateral partners in support of the R&D gaps identified as part of the broader PSVP program. To contact PSVP, email psvp@hq.dhs.gov.

First Responders Resource Group (FRRG)

S&T created the First Responder Resource Group (FRRG), made up of about 150 state, local, federal, and tribal first responders and subject-matter experts from across the country and internationally, and utilizes these experienced and knowledgeable responders to provide insight on issues they face, including response capability deficits they encounter, and to provide useful feedback on requirements for future solutions. This group provides S&T insight into the needs of our responders. The FRRG has championed several Law Enforcement (LE) based technologies that assist all responders such as the Law Enforcement ERAD Pre-Paid Card Reader for criminal investigations, render safe tactics, techniques, and procedures for Public Safety Bomb Technicians, Tactical Awareness Kit for a common tactical platform, laser eye protection, and improved ballistic protection during large crowd events. To contact the FRRG, email First.Responder@HQ.DHS.GOV.

Law Enforcement Related Science and Technology

S&T published the "Providing Police Backup Through Science and Technology" resource guide showcasing its law enforcement-related work. S&T programs support law enforcement through the development of technologies to combat financial crimes, child exploitation, cyber, narcotics, and other related crimes.

Detection Canine Research

Canines are an effective resource for detection operations. S&T's Detection Canine Program provides the Homeland Security Enterprise (HSE)—including DHS Components, SLTT, and campus agencies—with the tools, techniques, and knowledge to better understand, train, and deploy detection canines in their operational environment.

Border Security Research

DHS secures the borders, territorial waters, ports, terminals, waterways, and air, land, and sea transportation systems of the United States. S&T invests in border security research and development for technologies; provides solutions to prevent illicit movement and illegal entry or exit of people, weapons, dangerous goods, and contraband; works closely with border and immigration officials to understand how technology can help support their missions and overcome challenges; and manages risks posed by people and goods in transit.

Radiological/Nuclear Response and Recovery

S&T's National Urban Security Technology Laboratory (NUSTL) develops technical resources, tools, modeling, and guidance to help SLTTC public safety agencies initiate a response in the first minutes, hours, and days following radiological and nuclear incidents and support longer-term recovery needs. Three NUSTL-developed guidance documents that provide responders with tools and knowledge to prepare for and respond to radiological and nuclear incidents are below.

- Using Preventative Radiological Nuclear Detection Equipment for Consequence Management Missions Operational Job Aids describes procedures for the use of first responder preventive radiological/nuclear detection equipment in a response to a radiological material release.
- The Radiological Dispersal Device (RDD) Response Guidance Planning for the First 100 Minutes and accompanying videos both provide actionable guidance and annexed tools that can be used for local planning of an effective response to an RDD, that protects first responders and the public.
- The Nuclear Detonation Response Guidance: Planning for the First 72 Hours provides federal and SLTTCs with operational guidance on how to respond to a nuclear detonation in or near their jurisdiction in the first 72 hours of a nuclear detonation.

These science-based resources inform emergency planning and can be leveraged to shape response tactics for radiological and nuclear emergencies. Learn more about Radiological/Nuclear Response and Recovery Research & Development.

U.S. Secret Service National Threat Assessment Center (NTAC)

The U.S. Secret Service's NTAC produces operationally relevant research examining all forms of targeted violence, including domestic terrorism and mass-casualty attacks, along with school attacks, workplace violence, attacks against houses of worship, and other acts of targeted violence impacting communities across the nation. In January 2023, NTAC published its most comprehensive yearly analysis of mass attacks impacting public locations to date. In 2022, NTAC released a behavioral case study titled, Hot Yoga Tallahassee: A Case Study of Misogynistic Extremism. The case study was widely disseminated through federal, state, local, and private sector partners to stakeholders across the United States and is incorporated in NTAC training seminars for public safety professionals.

Training and Funding Opportunities

Training Opportunities

Federal Law Enforcement Training Centers (FLETC)

Through FLETC, DHS operates the largest law enforcement training institution in the country. FLETC prepares the federal law enforcement community to safeguard America's people, property, and institutions, and provides access to law enforcement training to SLTT, and campus law enforcement. In addition to basic training topics, FLETC training encompasses hundreds of advanced training programs including courses on active shooter/active threat; tactical medical; terrorism prevention; cybercrimes investigations; computer forensics; physical security; human trafficking awareness, and much more. Search available FLETC classes.

Office for Civil Rights and Civil Liberties' (CRCL) Fusion Center Training

State and major urban area fusion centers receive support from DHS and other federal partners through deployed personnel, training, technical assistance, technology, and grant funding. CRCL has dedicated personnel and resources to assist fusion center Civil Liberties and Privacy Officers (CLPOs), and those performing civil liberty and privacy functions in fusion centers. The assistance that CRCL provides includes direct regular communication between CRCL staff and fusion centers, CRCL acting as a liaison in facilitating subject matter guidance, and CRCL maintaining the new Fusion Center CLPO Community of Interest (COI) located within the HSIN. The COI shares model policies, training material, and best practices.

FEMA's National Training and Education Division (NTED)

FEMA's National Training and Education Division (NTED) provides funding and oversight for roughly 49 partners across the nation, who provide courses for first responders, emergency managers, and others in the community. In all, the NTED catalog includes 231 courses suited for law enforcement personnel. NTED also supports the Center for Homeland Defense and Security, focusing on assisting current and emerging leaders in Homeland Defense and Security to develop the policies, strategies, programs and organizational elements needed to defeat terrorism and prepare for and respond to natural disasters and public safety threats across the United States. Learn more about the National Preparedness Course Catalog.

FEMA’s Center for Domestic Preparedness (CDP)

The Center for Domestic Preparedness (CDP) provides free, advanced, all-hazards training to approximately 50,000 emergency responders annually from SLTT governments, and campus agencies, and on a cost-reimbursable basis for federal government, foreign governments, and private entities. The scope of training includes preparedness, protection, and response. The CDP is home to the Chemical, Ordnance, Biological, and Radiological Training Facility (COBRATF), the only site in the nation where civilian responders can train with toxic chemical and biological agents. Additional training venues include the Noble Training Facility (NTF), the nation’s only hospital dedicated solely to preparing healthcare communities for mass casualty events related to terrorist acts, and the Advanced Responder Training Complex (ARTC), a multi-use responder training facility that includes a simulated industrial park, subway station, and street scenes with businesses, offices, and warehouses.

I&A’s National Threat Evaluation and Reporting (NTER) Master Trainer Program (MTP)

The NTER Master Trainer Program (MTP) is a train-the-trainer initiative that certifies federal, state, local, tribal, territorial, and campus partners in the instruction of Behavioral Threat Assessment and Management (BTAM) techniques and best practices.

I&A’s Foundations of Targeted Violence Prevention eLearning

The NTER Program Office partnered with the Wisconsin Department of Justice and the Wisconsin Department of Public Instruction to release an eLearning module for all homeland partners on how to identify threatening or potentially concerning behaviors and where to report them, providing an opportunity for intervention to prevent targeted violence. It seeks to assist in preventing targeted violence by empowering community members to recognize threats or potentially concerning behaviors; understand what behaviors may be displayed by a person who is on a pathway to violence; learn where to report information of concern; understand how the information reported will be used to keep our community safe. Learn more about the Foundations of Targeted Violence Prevention eLearning.

Online Suspicious Activity Reporting (SAR) Training for Law Enforcement and Hometown Security Partners

The Nationwide SAR Initiative (NSI) training strategy is a multifaceted approach designed to increase the effectiveness of state, local, tribal, territorial, and campus law enforcement and public safety professionals and other frontline partners in identifying, reporting, evaluating, and sharing pre-incident terrorism indicators to prevent acts of terrorism. SAR has ten public-facing trainings for frontline officers and hometown security partners in recognizing what kinds of suspicious behaviors are associated with pre-incident terrorism activities, understanding how and where to report suspicious activity, while protecting privacy, civil rights, and civil liberties when documenting information. This training also provides information about integrating the Nationwide SAR Initiative (NSI) into your organization's operations.

Office for Bombing Prevention (OBP)

The Office for Bombing Prevention (OBP) offers training across multiple platforms to meet stakeholder needs. For instance, training is conducted by mobile training teams that conduct onsite training, in-residence at the FEMA Center for Domestic Preparedness (CDP), online through a virtual instructor-led training (VILT) platform, and through independent study training (IST) programs.

The Infrastructure Security Division (ISD)

Infrastructure Assessments and Analysis (IAA) works across the security enterprise to provide accredited training on technical tools and critical infrastructure security and resilience topics. The Program Training Branch now offers Fire as A Weapon training through multiple platforms to meet stakeholder needs via direct delivery on a in-person in a traditional classroom setting at a host site, or online through a virtual instructor-led training (VILT) platform. Fire as a Weapon is part of the PTB Threat Vector Series. This course covers threat risks and awareness, planning, prevention, and deterrence of fires to critical infrastructure as a single attack strategy or as part of a complex coordinated attack. The curriculum takes a closer look at the driving forces associated with intentional Fire as a Weapon incident and the risks and threats associated to national and critical infrastructure security. For more information email iaa-ptb-trainingrequests@cisa.dhs.gov.

Community Awareness Briefing (CAB)

The Community Awareness Briefing (CAB) is a one- to two-hour presentation that provides local communities an opportunity to learn about preventing targeted violence and terrorism and explore ways to prevent such threats at the local level. The CAB provides community members with information and tools to help them understand the threat of targeted violence and terrorism, and how they can prevent it by working with the whole community to develop violence prevention programs. Learn more about the Community Awareness Briefing by emailing CABBriefingRequests@hq.dhs.gov.

National Computer Forensics Institute (NCFI)

The National Computer Forensics Institute (NCFI), located in Hoover, Alabama, is the nation's premier federally funded training center committed to the instruction of state and local law enforcement officers, prosecutors, and judges in cybercrime investigations and cyber incident response.

NCFI empowers state and local law enforcement and the USSS network of Cyber Fraud Task Forces through provision of technical, hands-on training in network incident response and digital evidence process, to include applicable case law for high-tech crime prosecution.

CISA Tabletop Exercise Package (CTEP) Program

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. Each package is customizable and includes template exercise objectives, scenarios, and discussion questions as well as a collection of references and resources. Available scenarios cover a broad array of physical security and cybersecurity topics, such as natural disasters, pandemics, civil disturbances, industrial control systems, election security, ransomware, vehicle ramming, insider threats, active assailants, and unmanned aerial systems.

Resources from the Department of Justice's National Criminal Intelligence Resource Center

- Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies
- The Importance of Privacy, Civil Rights, and Civil Liberties Protections in American Law Enforcement and Public Safety
- Privacy, Civil Rights, and Civil Liberties Audit Guidance for State, Local, Tribal, and Territorial Intelligence Agencies
- Role of State and Local Law Enforcement at First Amendment Events Reference Card
- First Amendment Online Training

Funding Opportunities

Nonprofit Security Grant Program

The Nonprofit Security Grant Program (NSGP) provides funding to support facility hardening and other physical and cyber security enhancements for nonprofit organizations that are at high risk of a terrorist attack. Grant proposals must be submitted by an eligible nonprofit organization through each organization's State Administrative Agency (SAA), and law enforcement agencies are encouraged to partner with non-profit organizations to ensure a comprehensive submission. This partnership can take the form of a review of an organization's current security gaps, provision of local crime and threat information, and other advisory engagements.

Operation Stonegarden

Operation Stonegarden, a sub-component of the Homeland Security Grant Program (HSGP), provides funding to enhance cooperation and coordination among SLTT, and federal law enforcement agencies to jointly enhance security along our borders. Entities eligible for funding are state, local, and tribal law enforcement agencies that are located along the border of the United States, and which have active, ongoing U.S. Border Patrol (USBP) operations coordinated through a CBP office. Those entities work with their relevant SAA to submit applications. Funding can be applied towards overtime, hiring, equipment, and training. USBP hosted 416 engagements in FY 2022, and DHS provided $90 million in grant funding.

Port Security Grant Program

The Port Security Grant Program provides funding to state, local, and private-sector partners to help protect critical port infrastructure from terrorism, enhance maritime domain awareness, improve port-wide maritime security risk management, and maintain or reestablish maritime security mitigation protocols that support port recovery and resiliency capabilities. Eligible applicants include but are not limited to port authorities, facility operators, and state and local government agencies. Funding is directed towards the implementation of Area Maritime Security Plans, Facility Security Plans, and Vessel Security Plans among port authorities, facility operators, and state and local government agencies that are required to provide port security services.

State Homeland Security Program

The State Homeland Security Program, a sub-component of the Homeland Security Grant Program (HSGP), provides funding to support the implementation of risk-driven, capabilities-based state homeland security strategies to assist efforts in preventing, protecting against, mitigating, and responding to acts of terrorism and other threats. Every year, each state and territory is required to allocate a certain percentage of their funding towards law enforcement terrorism prevention activities. Funding for this grant program is determined utilizing a risk-based formula and is administered by the State Administrative Agencies (SAA).

State and Local Cybersecurity Grant Program

The State and Local Cybersecurity Grant Program provides funding to eligible entities to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, state, local, or tribal governments. The State and Local Cybersecurity Grant provides $1B in funding over four (4) years.

Targeted Violence and Terrorism Prevention Grant Program

The Targeted Violence and Terrorism Prevention (TVTP) Grant Program provides funding for SLTTC governments, nonprofits, and institutions of higher education with funds to establish or enhance capabilities to prevent targeted violence and terrorism.

Transit Security Grant Program

The Transit Security Grant Program (TSGP) provides funding to eligible public transportation systems (which include intra-city bus, ferries, and all forms of passenger rail) to protect critical transportation infrastructure and the traveling public from terrorism, and to increase transportation infrastructure resilience. Certain law enforcement agencies are eligible as subrecipients to transit systems if they provide dedicated transit security support to that system. Agencies eligible for the TSGP funding are determined based upon daily unlinked passenger trips (ridership) and transit systems that serve historically eligible Urban Area Security Initiative (UASI) urban areas.

Tribal Homeland Security Grant Program

The Tribal Homeland Security Grant Program provides funding to tribal nations to implement preparedness initiatives to help strengthen the nation against risk associated with potential terrorist attacks and other hazards. Criteria for application eligibility includes federally-recognized Tribes that; operate a law enforcement or emergency response agency with the capacity to respond to calls for law enforcement or emergency services; are located on or near (100 miles) an international border or a coastline bordering an ocean (including the Gulf of Mexico) or international waters; are located within 10 miles of a system or asset included on the prioritized critical infrastructure list established under section 2214(a)(2) of the Homeland Security Act of 2002, as amended (6 U.S.C. § 664(a)(2) or has such a system or asset within its territory; as well as additional criteria.

Urban Area Security Initiative

The Urban Area Security Initiative, a sub-component of the Homeland Security Grant Program (HSGP), provides funding to enhance regional preparedness and capabilities in high-threat, high-density areas to assist efforts in preventing, protecting against, mitigating, and responding to acts of terrorism and other threats. Every year, each high-risk urban area is required to allocate a certain percentage of their funding towards law enforcement terrorism prevention activities. Funding for this grant is determined utilizing a risk-based formula and is administered by the SAAs.

U.S. Coast Guard Grants Management Branch (BSX-22)

The Coast Guard Grants Management Branch provides financial oversight to all Recreational Boating Safety Grant Awards. This includes the posting of the Notice of Funding Opportunity (NOFO), obligations, grantee payments, USAspending.gov uploads, and the scheduling of grants management training. There are three Grant Programs funded by the Division of Boating Safety.

Additional Grant Opportunities through DHS

Learn more about additional grant opportunities through DHS.

Additional Grant Opportunities through the Department of Justice

Learn more about additional grant opportunities through the Department of Justice.

Other Resources

DHS Office for State and Local Law Enforcement (OSLLE)

OSLLE leads the coordination of DHS-wide policies related to SLTTC law enforcement's role in preventing, preparing for, protecting against, and responding to natural disasters, acts of terrorism, and other man-made disasters within the United States. OSLLE also serves as the primary liaison between DHS and non-federal law enforcement agencies across the country. OSLLE ensures that SLTTC law enforcement has DHS operational and strategic support, as well as access to DHS resources to help counter current and emerging threats. To learn more, please contact: OSLLE@hq.dhs.gov.

S&T's National Urban Security Technology Laboratory (NUSTL)

S&T's National Urban Security Technology Laboratory (NUSTL) assesses the performance and suitability of Counter-Unmanned Aircraft Systems (C-UAS) technologies across a variety of law enforcement applications and provides technical expertise to law enforcement partners on available technologies useful for countering malicious UAS. To detect, track, and identify UAS and effectively respond to these threats in a timely manner, law enforcement entities require specialized equipment and knowledge based on their operating environment and operational missions. Learn more in the C-UAS Technology Guide and Questions to Ask When Researching C-UAS.

Responding to Drone Calls: Guidance for Emergency Communications Centers

As drone activity continues to increase in the United States, Emergency Communications Centers (ECCs) or Public Safety Answering Points (PSAPs) may experience an increase in drone-related calls. ECCs should understand the distinctions between proper and improper drone activity and collect the information needed to inform potential law enforcement response. This guidance provides an overview of both safe and suspicious drone flight activity and a suggested script that may be used during a drone-related call.

Unauthorized Drone Activity Over Sporting Venues

There have been recent drone sightings that have prompted game delays at sporting venues, highlighting concerns of unauthorized drone activity in the new spectator-restricted environment. Most instances involve fans seeking real-time game footage. However, malicious actors may utilize drones to disrupt, harass, or even cause physical injury or destruction of property. Regardless of intent, unauthorized drone activities pose a potential risk. This resource presents options for consideration by sporting venue owners and operators to prevent, protect from, and respond to unauthorized drone activity.

Tailored Assessments and Technical Requests

DHS S&T's Probabilistic Analysis for National Threats, Hazards, and Risks (PANTHR) program leverages its annual Chemical, Biological, Radiological, and Nuclear (CBRN) Strategic Risk Analysis results to provide customer and mission specific tailored analyses and technical requests to a variety of interagency and SLTTC partners. These tailored analyses allow SLTTC partners to make risk informed decisions related to medical countermeasure investments, resource prioritization, and much more.

U.S. DEPARTMENT OF
HOMELAND SECURITY