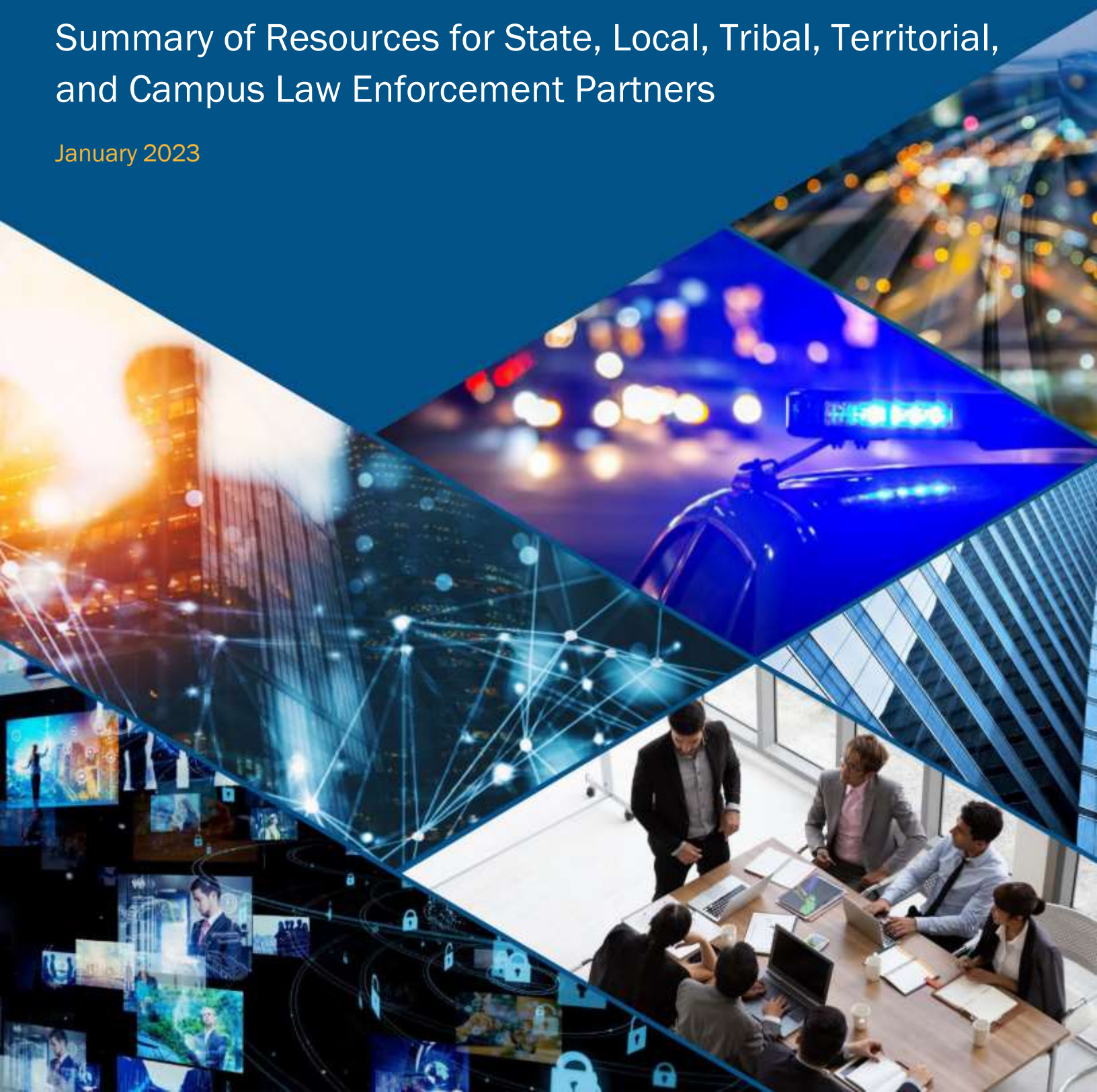
Homeland Security

U.S. DEPARTMENT OF HOMELAND SECURITY

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

January 2023



Homeland Security

Dear Law Enforcement Partners:

The Department of Homeland Security is proud to support and serve alongside you as you perform the noble work of the law enforcement profession. We are committed to ensuring you have the tools, resources, and support you need to continue to keep communities across our country safe. This guide highlights many of the Department's resources available to you, including training and grant opportunities, to increase our nation's ability to prevent acts of violence and increase our resilience to evolving threats.

To learn more, please contact the DHS Office for State and Local Law Enforcement at oslle@hq.dhs.gov. Thank you for your continued partnership and service to our nation.

Sincerely,

Alejandro N. Mayorkas
Secretary

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. Learn more.

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. Learn more.

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.

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 "If You See Something, Say Something®" message in their respective communities. Learn more.

Bombing Prevention

CISA, through its Office for Bombing Prevention (OBP), leads DHS's efforts to enhance our country'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 law enforcement entities. OBP offers specialized resources for those who have an official role in planning for or responding to bomb threats.

Preparedness and Prevention (continued)

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. Learn more.

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, including through its Hometown Security program. Learn more.

DHS Special Events Program

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 the chaos, being prepared can play an integral role in mitigating the impacts of an incident. 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. Learn more.

DHS Counter-IED Capabilities Assessment (CCA)

The Counter-IED Capabilities Assessment (CCA) is an assessment tool managed by CISA's OBP. OBP uses a consistent and repeatable methodology to assess and analyze the capabilities of units with a counter-IED mission throughout the United States. CCA assessments measure the capabilities of and identify gaps in Personnel, Organization, Equipment, Training, and Exercises (POETE) required for effective prevention, protection, and response to IED threats. CCAs can be used in many ways to include:

- First responder specialty teams use the CCA to assess and address internal capabilities and gaps
- Homeland Security Advisors and emergency management officials use CCA in resource allocation to sustain or enhance capabilities
- Grant writers and emergency planners use CCA to develop investment justifications that support State homeland security strategies and address POETE gaps

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 1) Video Analytics 2) Tactical Eyewear 3) Laser Protective Eyewear 4) Communications Equipment 5) Body Armor. Learn more.

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 state, local, tribal, territorial, campus, 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.

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, state, local, tribal, territorial, and campus partners 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.

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. Learn more.

Information and Intelligence Sharing (continued)

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, state, local, tribal, territorial (SLTT), campus, 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 SLTT 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 SLTT 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, state, local, tribal, and territorial Emergency Services Sector partners tools to prevent, protect from, respond to, 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 state, local, tribal, territorial (SLTT) 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.

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. Learn More.

Information and Intelligence Sharing (continued)

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

CISA also funds the MS-ISAC that is free for state, local, tribal, territorial, and campus agencies to join. CISA encourages SLTT agencies to sign up to receive their free services and capabilities, as well as receive time sensitive alerts and information. Learn More.

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, state, local, tribal, territorial, 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.

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.

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. Learn more.

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 and sign up for cybersecurity alerts.

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 state, local, tribal, and territorial 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.

"*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.

Cyber Fraud Task Forces

The U.S. Secret Service (USSS) operates Cyber Fraud Task Forces (CFTFs) to prevent, detect, and mitigate complex cyber-enabled financial crimes, with the goal of convicting the most harmful perpetrators. CFTFs, the focal point of USSS cyber investigative efforts, are partnerships between USSS, other law enforcement agencies, prosecutors, private industry, and academia. The strategically located CFTFs combat cybercrime through prevention, detection, mitigation, and investigation. Learn more.

Cybersecurity (continued)

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 risk to both physical security and cybersecurity—each can be targeted, separately or simultaneously, to result in compromised systems and/or infrastructure. When physical security and cybersecurity divisions operate in siloes, they lack a holistic view of security threats targeting their enterprise. Learn more.

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

- 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. Learn more.

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. Learn more.

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. Learn more.

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. Learn more.

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. Learn more.

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. 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.

Protective Security Advisors (PSAs)

PSAs proactively engage with federal, state, local, tribal, territorial, and campus partners and the private sector to protect critical infrastructure. These subject matter experts are trained to identify vulnerabilities and mitigate risk and are available to advise and assist organizations that have historically been targeted for violence. PSAs frequently partner with 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. Learn more.

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. Learn more.

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.

Chemical Facility Anti-Terrorism Standards (CFATS)

CISA's CFATS program identifies and regulates high-risk chemical facilities to ensure security measures are in place to reduce the risk of certain hazardous chemicals being weaponized. CFATS is vital to our nation's economy. Through the CFATS program, CISA ensures the federal government, the private sector, and members of the community, including law enforcement, hazmat, and first responders reduce the risk of hazardous chemicals of being weaponized. Learn more.

ChemLock

CISA's ChemLock program was launched in 2021 to provide no-cost voluntary services and tools to facilities that possess dangerous chemicals. The ChemLock program provides chemical security guidance documents, fact sheets, and flyers as well as training, on-site security assessments, and exercises/drills with new products and services being added regularly. Learn more.

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.

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 JCDC—the Joint Cyber Defense Collaborative—to unify cyber defenders from organizations worldwide. This diverse team proactively gathers, analyzes, and shares actionable cyber risk information to enable synchronized, holistic cybersecurity planning, cyber defense, and response. Learn more.

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. Learn more.

School Safety and Security

School Safety and Security Resources

CISA's K-12 School Security Guide (3rd Edition) and School Security Assessment Tool (SSAT) demonstrates how a layered, systems-based approach to school physical security planning can help schools create safe and secure learning environments. 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. Learn more.

SchoolSafety.gov

SchoolSafety.gov was created by the Departments of Homeland Security, 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. Learn more.

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. Learn more.

National Threat Assessment Center (NTAC)

The 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. Learn more.

Human Trafficking: Forced Labor and Sex Trafficking

DHS Center for Countering Human Trafficking

The DHS Center for Countering Human Trafficking 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, 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. Learn more.

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, state, local, tribal, territorial, 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 Continued Presence, please see the Continued Presence Toolkit which also provide instructions on how to request Continued Presence. Learn more.

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

Victims of human trafficking and other serious crimes, including domestic violence, sexual assault, and stalking, who assist law enforcement may qualify for T or U nonimmigrant status, also known as the T and U visas. U.S. Citizenship and Immigration Services (USCIS) has developed the following resources for federal, state, local, tribal and territorial law enforcement, judges, family protective services, and other certifying agencies, which 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.

USCIS also provides technical assistance to certifying officials 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.*

Human Trafficking: Forced Labor and Sex Trafficking (continued)

Blue Campaign's Law Enforcement Training and Awareness-Raising Resources

The Blue Campaign is a national public awareness campaign designed to educate the public, law enforcement, and other industry partners to recognize indicators of human trafficking and how to appropriately respond to potential cases. 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.

"Concern" Law Enforcement Victim-Centered Approach Virtual Training

The Blue Campaign just completed a new 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 judgment. Learn more.

Human Trafficking Response Guide for School Resource Officers

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.

U.S. Secret Service (USSS) Programs to Combat Human Trafficking and Child Exploitation

USSS, 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. USSS invites employees to become specially trained by the NCMEC and provide presentations to the community. In FY22, the USSS provided over 300 CSP presentations, reaching approximately 20,000 individuals. To request a CSP presentation, contact your local U.S. Secret Service field office or email fsdncmec@usss.dhs.gov. USSS values its partnership with the NCMEC. Learn more.

Human Trafficking: Forced Labor and Sex Trafficking (continued)

U.S. Secret Service (USSS) Forensic Resources

USSS combats human trafficking and child exploitation by providing NCMEC and other law enforcement agencies forensic support in any missing or exploited child case.

These forensic capabilities include polygraph examinations, video and audio enhancement, speaker identification, questioned documents, latent prints, composite sketches, and geospatial information systems. For forensic support of missing or exploited children's cases, please contact your local USSS Field Office. Learn more.

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. Learn more.

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. To accomplish this, S&T leverages federally funded universities and R&D centers, industry, national laboratories, and in-house subject matter experts in fields such as Countering Weapons of Mass Destruction and Cyber Security as well as emerging threats such as Counter Unmanned Aircraft Systems. Learn more.

First Responders Resource Group

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 bomb squad 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. Learn more.

Law Enforcement Related Science and Technology

In January 2022, 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. S&T also offers terrorism prevention-specific resources. Learn more.

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, state, local, tribal, territorial, and campus agencies—with the tools, techniques, and knowledge to better understand, train, and deploy detection canines in their operational environments. Learn more.

Research and Development (continued)

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. Learn more.

Radiological/Nuclear Response and Recovery

S&T's National Urban Security Technology Laboratory (NUSTL) develops technical resources, tools, modeling, and guidance to help state, local, tribal, and territorial public safety agencies initiate a response in the first minutes, hours, and days following radiological and nuclear incidents and support longer-term recovery needs. These science-based resources inform emergency planning and can be leveraged to shape response tactics for radiological and nuclear emergencies. Learn more.

National Threat Assessment Center (NTAC)

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 will publish 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. Learn more.

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 state, local, tribal, territorial, 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 classes. Learn more.

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 Homeland Security Information Network (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. The National Cybersecurity Preparedness Consortium provides more than 40 courses to improve the capabilities and capacity for cybersecurity events. Learn more.

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 state, local, tribal, territorial 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. Learn more.

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. Learn more.

Training and Funding Opportunities (continued)

Training Opportunities (continued)

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, and territorial 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. Learn more.

Office for Bombing Prevention (OBP)

OBP offers bombing prevention training through multiple platforms to meet stakeholder needs via direct delivery, in-person in a traditional classroom setting or 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). Learn more.

Community Awareness Briefing (CAB)

The Community Awareness Briefing (CAB) is a two-hour presentation that provides a foundation for communities across the country to learn about prevention efforts and radicalization to violence. The program provides communities with information and tools that are available to assist them with understanding the issues and learning more about how they can prevent targeted violence and terrorism within their communities. Learn more.

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 U.S. Secret Service's 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. Learn more.

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

Training and Funding Opportunities (continued)

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. Learn more.

Operation Stonegarden

Operation Stonegarden, a sub-component of the Homeland Security Grant Program (HSGP), provides funding to enhance cooperation and coordination among state, local, tribal, territorial, 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 US Border Patrol 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. Border Patrol hosted 416 engagements in FY22, and DHS provided $90 million in grant funding. Learn more.

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. Learn more.

State Homeland Security Program

The State Homeland Security Program, a sub-component of 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 SAAs. Learn more.

Training and Funding Opportunities (continued)

Funding Opportunities (continued)

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. Learn more.

Targeted Violence and Terrorism Prevention Grant Program

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

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. Learn more.

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. Learn more.

Urban Area Security Initiative

The Urban Area Security Initiative, a sub-component of 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. Learn more.

Training and Funding Opportunities (continued)

Funding Opportunities (continued)

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

The 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. Learn more.

Additional Grant Opportunities through DHS

Learn more.

Additional Grant Opportunities through the Department of Justice

Learn more.

Other Resources

DHS Office for State and Local Law Enforcement (OSLLE)

OSLLE leads the coordination of DHS-wide policies related to state, local, tribal, territorial, and campus 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) 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. Learn more.

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. Learn more.

Key Tips

- Strengthen relationships, build trust, and stay engaged with community members and leaders from every level of government.
- Consider designating a liaison to establish relationships with key stakeholders in targeted communities, such as Asian American Native Hawaiian and Pacific Islander (AANHPI); Black; Hispanic; Jewish; Lesbian, Gay, Bi-Sexual, Transgender, Queer, Intersex, Asexual, and more (LGBTQIA+); and Middle East and North African. This designated liaison can be a community member or law enforcement officer with cultural competency and sensitivity training.
- Be proactive and encourage the visibility of uniformed officers within communities to assist with easing tensions and preventing incidents.
- Engage with community members and non-governmental organizations to educate the public about crime prevention and how to report crimes or suspicious activity.