



Homeland Security

U.S. DEPARTMENT OF HOMELAND SECURITY

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

April 2022





Homeland Security



Dear Law Enforcement Partners:

The Department of Homeland Security is proud to support and work alongside you as you perform the noble work of the law enforcement profession.

You work on the front lines every day, at great personal risk, to keep our communities safe. We are committed to ensuring you have the tools, resources, and support you need to continue doing so successfully. This guide highlights many of the resources available to you, including training and grant opportunities, to increase our nation's resilience to evolving threats. If you would like 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,

A handwritten signature in blue ink that reads "Alejandro N. Mayorkas".

Alejandro N. Mayorkas
Secretary of Homeland Security

Table of Contents

<i>Preparedness and Prevention.....</i>	<i>4</i>
<i>Information and Intelligence Sharing.....</i>	<i>6</i>
<i>Cybersecurity.....</i>	<i>7</i>
<i>Critical Infrastructure Protection.....</i>	<i>9</i>
<i>School Safety and Security.....</i>	<i>10</i>
<i>Human Trafficking, Forced Labor, and Sex Trafficking.....</i>	<i>11</i>
<i>Training and Funding Opportunities.....</i>	<i>12</i>
<i>Key Tips.....</i>	<i>15</i>



Preparedness and Prevention

DHS Center for Prevention Programs and Partnerships (CP3)

CP3 provides communities with the resources and tools – including technical, financial, and educational assistance – to help prevent individuals from radicalizing to violence. [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 their facilities. 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 [If You See Something, Say Something®](#) campaign partners include state, local, tribal, and territorial governments who are essential to increasing awareness about how to report suspicious activity to prevent acts of violence. [Learn more.](#)

Bombing Prevention

CISA, through its Office of 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. [Learn more.](#)

National Threat Evaluation and Reporting Program

The National Threat Evaluation and Reporting Program (NTERP) is a collaborative effort between DHS and federal, state, local, tribal, territorial, and campus partners. The NTERP advances our partner's ability to identify, investigate, assess, report, and share tips and leads linked to emerging homeland security threats, and receive support, resources, and training. Learn more by reviewing the [Behavioral Approach to Violence Prevention Summary](#) and [NTERP Fact Sheet](#). Contact the NTERP at NTER.MTP@hq.dhs.gov.

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.](#)



Preparedness and Prevention (continued)

DHS Special Events Program

The DHS Special Events Program (SEP) manages the National Special Event Data Call (NSEDG), 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 NSEDG by state and local authorities each year. The primary data collection period opens the first week of August and remains open for six weeks before closing in mid-September. The SEP continues to accept event submissions throughout the year as “short notice events” – those submitted outside the six-week data call period. All events submitted to the NSEDG receive a Special Events Assessment Rating (SEAR) that is applied using a risk-based analytical approach. Questions about SEAR or the National Special Events Data Call 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. In the midst of the chaos, anyone can play an integral role in mitigating the impacts of an active shooter incident. [Learn more](#).



Information and Intelligence Sharing

DHS Office of Intelligence and Analysis (I&A)

[I&A](#) is the only member of the Intelligence Community statutorily charged with bi-directional information and intelligence sharing with state, local, tribal, territorial (SLTT) and private sector partners. DHS has renewed its commitment to sharing actionable and timely information and intelligence with these partners at the lowest classification level possible. I&A partners have access to the [National Threat Evaluation and Reporting \(NTER\) Program](#), which provides certification in Behavioral Threat Assessment techniques and best practices to reduce the threat of targeted violence. [Learn more.](#)

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, 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 will launch in April 2022 the INTEL App, which will enable 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 and critical infrastructure owners and operators partners with a secure platform to share intelligence and information related to critical infrastructure protection.

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.](#)

FBI National Incident-Based Reporting System (NIBRS)

The FBI's NIBRS identifies when and where crime takes place, what form it takes, and the characteristics of its victims and perpetrators. This system provides greater specificity regarding reporting offenses, collects more detailed information, helps give greater context to specific crime problems, and provides increased analytic flexibility. This tool helps law enforcement better define the resources it needs to fight crime. [Learn more.](#)



Information and Intelligence Sharing (continued)

DHS National Terrorism Advisory System (NTAS) Advisories

Through the NTAS, DHS provides public and private sector partners and the public with information regarding the threat landscape facing the United States and resources for how to stay safe. In alignment with its renewed commitment to sharing actionable and timely information and intelligence with the broadest audience possible, DHS has issued five NTAS Bulletins since January 2021. [Read the current NTAS Bulletin here](#) and [sign-up to receive future NTAS advisories here](#).

DHS Technical Resource for Incident Prevention (TRIPwire)

TRIPwire is DHS's 24/7 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 combines information and analysis to help users anticipate, identify, and prevent improvised explosive device (IED) incidents 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.

Combating 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](#).

CISA's Shields Up Campaign

While there are currently no specific or credible cyber threats to the U.S. homeland, Russia's unprovoked attack on Ukraine may impact organizations both within and beyond the region. As the nation's cyber defense agency, CISA stands ready to help organizations prepare for, respond to, and mitigate the impact of cyber attacks. 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 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, CISA has compiled a catalogue of related free services and resources. [Learn more](#).

Cyber Fraud Task Forces

The U.S. Secret Service operates Cyber Fraud Task Forces, which prevent, detect, and mitigate complex cyber-enabled financial crimes, with the goal of convicting the most harmful perpetrators. [Learn more](#).

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

ICE HSI 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 Forensic 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. For requests for assistance, agencies should contact their local HSI office.



Cybersecurity (continued)

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 Cyber Crimes Center (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 Homeland Security Investigations (HSI) Child Exploitation Investigations Unit (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.

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.](#)



Critical Infrastructure Protection

CISA Critical Infrastructure Vulnerability Assessments

CISA's Infrastructure Security Division conducts voluntary specialized field assessments to identify vulnerabilities, interdependencies, capabilities, and cascading effects of impacts on U.S. critical infrastructure. [Learn more.](#)

CISA 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.](#)

Chemical Facility Anti-Terrorism Standards (CFATS)

Chemicals are vital to our nation's economy and reducing the risk of hazardous chemicals from being weaponized is a shared commitment between the federal government, the private sector, and members of the community, including law enforcement, hazmat, and first responders. 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. [Learn more.](#)



School Safety and Security

CISA's School Safety and Security Resources

CISA's [K-12 School Security Guide \(3rd Edition\)](#) and [School Security Assessment Tool](#) demonstrates how a systems-based approach to school physical security planning can help schools create safe and secure learning environments. This guide focuses on the most common incidents of crime and violence that K-12 schools in the United States face today. CISA's School Safety and Security webpage offers additional resources. [Learn more.](#)

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

The NTAC provides public safety research and guidance, and its multidisciplinary team of social science researchers and regional program managers 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. The NTAC created an [operational guide](#) with actionable steps to develop comprehensive targeted violence prevention plans for conducting threat assessments in schools, [examined 67 averted attacks](#) at K-12 schools from 2006-2018 planned by students, and [analyzed 41 attacks](#) perpetrated by students at K-12 from 2008-2017. [Learn more.](#)

FEMA's National Training and Education Division Course Catalogue

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



Human Trafficking, Forced Labor, and Sex Trafficking

Blue Campaign: 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](#).

Continued Presence Program

DHS through the Center for Countering Human Trafficking 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 request Continued Presence assistance, please email: ContinuedPresence@ccht.dhs.gov. [Learn more](#).

USCIS: U and T Visas for Victims of Human Trafficking and Other Serious Crimes

Qualifying victims of human trafficking and other serious crimes, including domestic violence, sexual assault, and stalking, who assist law enforcement may qualify for immigration relief, with help from law enforcement and other certifying agencies at the federal, state, local, or tribal level. USCIS has developed resources for law enforcement, judges, family protective services, and other certifying agencies who may be certifiers for individuals applying to USCIS for U or T nonimmigrant status, also known as the U and T visas. [Learn more](#).

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](#).



Training and Funding Opportunities

Training Opportunities

Federal Law Enforcement Training Centers (FLETC)

Through FLETC, DHS operates the largest law enforcement training program in the country. FLETC equips our law enforcement partners with the skills they need to keep our communities safe. Courses include how to safely operate firearms, drive safely in emergency situations, conduct overcover operations, collect and inspect evidence, and much more. [Learn more.](#)

FEMA's National Training and Education Division (NTED)

The NTED provides more than 150 courses to better prevent, protect, respond to, and recover from manmade and natural catastrophic events. [Learn more.](#)

FEMA's Center for Domestic Preparedness

The Center for Domestic Preparedness provides advanced, all-hazards training to approximately 50,000 emergency responders annually from state, local, tribal, and territorial governments, and other public and private sector entities. [Learn more.](#)

Funding Opportunities

Nonprofit Security Grant Program

The Nonprofit Security Grant Program (NSGP) provides funding to support target hardening and other physical security enhancements for nonprofit organizations that are at high risk of a terrorist attack. Although grant proposals must be submitted by an eligible nonprofit organization, law enforcement agencies are encouraged to partner with non-profit organizations to ensure a comprehensive submission. [Learn more.](#)

Operation Stonegarden

Operation Stonegarden provides funding to enhance cooperation and coordination among state, local, tribal, territorial, and federal law enforcement agencies to jointly enhance security along our borders. [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. [Learn more.](#)

State Homeland Security Program

The State Homeland Security Program (SHSP) provides funding to support the implementation of risk-driven, capabilities-based state homeland security strategies to assist efforts in preventing, protecting against, mitigation, responding to, and recovering from acts of terrorism and other threats. [Learn more.](#)



Training and Funding Opportunities (continued)

Targeted Violence and Terrorism Prevention Grant Program

The Targeted Violence and Terrorism Prevention Grant Program (TVTP) provides funding for state, local, tribal, and territorial partners to implement innovative solutions for preventing targeted violence and terrorism and enhance local threat assessment and management capabilities. [Learn more.](#)

Transit Security Grant Program

The Transit Security Grant Program 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 travelling public from terrorism, and to increase transportation infrastructure resilience. [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. [Learn more.](#)

Urban Area Security Initiative

The Urban Area Security Initiative (UASI) provides funding to enhance regional preparedness and capabilities in high-threat, high-density areas to assist efforts in preventing, protecting against, mitigating, responding to, and recovering from acts of terrorism and other threats. [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 (SLTTC) law enforcement's role in preventing, preparing for, protecting against, and responding to natural disasters, acts of terrorism, and other man-made disaster within the United States, and 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.



Training and Funding Opportunities (continued)

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 through research and development, technical expertise, technology, and funding. In January 2022, S&T published the "[Providing Police Backup Through Science and Technology](#)" resource guide showcasing its law enforcement-related work. S&T also offers [terrorism prevention-specific resources](#). [Learn more](#).

Unmanned Aircraft Systems (UAS): Considerations for Law Enforcement Action

Unmanned aircraft systems (UAS), also known as unmanned aerial vehicles (UAV) or drones, are aircraft that are controlled by an operator remotely or programmed to fly autonomously. While UAS in and of themselves are benign, negligent, reckless, wantonly dangerous, or nefarious use can seriously threaten the personal safety of emergency services personnel and the public, as well as obstruct law enforcement operations. When law enforcement action is taken against UAS and their operators, law enforcement personnel need to be aware of several Federal statutes that that can affect their engagement. [Learn more](#).

U.S. Secret Service Analysis of Mass Attacks

The U.S. Secret Services produced a report that examines mass attacks impacting public or semi-public locations where three or more individuals were injured or killed. [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](#).

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](#)
- Training video: [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](#)



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 Hispanic, Jewish, AANHPI, LGBTQAI+, and Black communities. 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.



Homeland
Security