Homeland Security

DHS State and Local Law Enforcement Resource Catalog

Volume VI May, 2018

Intentional blank page. Please continue to the next page.

Letter from the Office for State and Local Law Enforcement

May 25, 2018

Dear Law Enforcement Partners:

Homeland security begins with hometown security. The U.S. Department of Homeland Security (DHS) strives to provide its state, local, tribal, and campus law enforcement partners with the latest tools, information, and resources to aid them in protecting their communities . With the release of the *DHS State and Local Law Enforcement Resource Catalog, Volume VI*, we are pleased to continue assisting the brave men and women serving in state, local, tribal, and campus law enforcement agencies across the country. Future iterations of this resource catalog will be updated and disseminated on an annual basis.

The *DHS State and Local Law Enforcement Resource Catalog* is a one-stop shop for non-federal law enforcement. This document summarizes and provides links to training, publications, newsletters, programs, and services available from the offices and components across the Department (e.g., U.S. Immigration and Customs Enforcement, Transportation Security Administration) to our law enforcement partners.

At DHS, we are continually developing new programs and resources to assist state, local, tribal, and campus law enforcement. If you cannot find what you are searching for in this catalog, please do not hesitate to contact the Office for State and Local Law Enforcement for additional assistance.

The Office for State and Local Law Enforcement endeavors to enhance the support that DHS provides to our law enforcement partners. We hope this catalog will assist you in your efforts to keep our communities safe, secure, and resilient.

Sincerely,

Office for State and Local Law Enforcement
U.S. Department of Homeland Security

Office for State and Local Law Enforcement

Overview

In 2007, on the recommendation of the 9/11 Commission, Congress created the Office for State and Local Law Enforcement (OSLLE) to lead 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.

Contact OSLLE

Phone: 202-282-9545

Email: OSLLE@hq.dhs.gov

Website: http://www.dhs.gov/office-state-and-local-law-enforcement-oslle

Responsibilities

- Serve as primary Department liaison to state, local, tribal, and territorial law enforcement;
- Advise the Secretary on the issues, concerns, and recommendations of state, local, tribal, and territorial law enforcement;
- Keep the law enforcement community informed about Department-wide activities and initiatives such as "If You See Something, Say Something™", the Blue Campaign, Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI), and the Department's efforts in Countering Violent Extremism;
- Identify and respond to law enforcement challenges that affect homeland security;
- Coordinate with the Office of Intelligence and Analysis to ensure timely coordination and distribution of intelligence and strategic information to state, local, tribal, and territorial law enforcement; and
- Work with the Federal Emergency Management Agency to ensure that law enforcement and terrorism-focused grants to state, local, tribal, and territorial law enforcement agencies are appropriately focused on terrorism prevention activities.

Helping to Build a Safe, Secure, and Resilient Nation

Table of Contents

Department-Wide Resources

Active Shooter Preparedness Resources. The Department of Homeland Security offers a number of resources to state and local law enforcement for responding to active shooter incidents.

Active Shooter Preparedness resources include a desk reference guide; a poster; and a pocket-size reference card to address how employees, managers, training staff, and human resources personnel can mitigate the risk of, and appropriately react in the event of, an active shooter situation. To access all of these resources, visit http://www.dhs.gov/active-shooter-preparedness. Materials also are available in Spanish.

The Federal Law Enforcement Training Centers (FLETC) offer tuition-free or low-cost training courses, including an Active Shooter Threat Training Portfolio that includes the following training programs:

- *Active Shooter Threat Training Program (ASTTP)* – covers fundamental/basic skills;
- *Active Shooter Threat Instructor Training Program (ASTITP)* – instructor level, "train-the-trainer" program;
- *Basic Tactical Medical Instructor Training Program (BTMITP)* – the law enforcement officer will gain knowledge and skills necessary to mitigate the loss of their life or the life of another while in an active threat environment. The skills will address treating life threatening injuries in an austere environment with limited equipment, lack of medically trained personnel, and prolonged time to evacuation; and

- *Tactical Medical First Responder (8 hour) Training Program (TMFR).*

These training programs are designed to provide law enforcement officers with the threat awareness, analytical knowledge, tactical skills, and emergency first aid skills that are needed to successfully serve as a law enforcement first responder in an active shooter/threat situation. The programs are conducted at selected venues throughout the country, hosted by a local law enforcement agency, or at one of FLETC's training delivery points, which are located in Artesia, NM; Charleston, SC; Cheltenham, MD; and Glynco, GA. To learn more about FLETC training courses available to state, local, tribal, and campus law enforcement, and for contact information, visit https://www.fletc.gov/state-local-tribal or contact stateandlocaltraining@dhs.gov.

Additionally, the Science and Technology Directorate (S&T) Enhanced Dynamic Geo-Social Environment (EDGE) Virtual Training platform provides a free virtual training environment for all first responders to enhance cross-disciplinary coordination and communications. See more on page 54.

Within the Homeland Security Information Network (HSIN), the Joint DHS and Federal Bureau of Investigation (FBI) Countering Violent Extremism (CVE) and Active Shooter (AS) Web Portal provides a forum to share Unclassified For Official Use Only (FOUO), Sensitive but Unclassified (SBU), and Law Enforcement Sensitive (LES) information with anyone who is a sworn, full-time, salaried, law enforcement officer (federal, state, or local); federal employee affiliated with the criminal justice system or intelligence communities; military personnel; and governmental agencies associated with infrastructure protection of the United States. The Portal also shares Unclassified FOUO or SBU information with private sector partners, civilian security personnel, corporate executives, academic institution employees, first responders (including firefighters and emergency medical services), international partners, religious leaders, and other state and local partners that are not law enforcement personnel, as appropriate. The portal provides users and training practitioners with accurate, appropriate, and relevant CVE and Active

Shooter training development resources, subject matter expert information, and outreach initiatives. It also has forums to provide feedback, products useful to others, and allows participants to ask questions concerning CVE or the Active Shooter Program. Persons with a job-related duty, public service interest, or who support a CVE and/or Active Shooter program can request access into this Portal. Work-related information is needed to ensure members are provided the appropriate accesses and their work activities justify a need to know. This information is used to nominate the user into HSIN. The user will then receive an email to validate their information. To request access, email: cveasportal@hq.dhs.gov. Provide the following information in the body of the email:

- Full Name;
- Place of Employment;
- Job Title;
- Work Email Address;
- Work Phone Number;
- Short Job Description as it Relates to CVE or Active Shooter.

Blue Campaign to Fight Human Trafficking. DHS is responsible for investigating human trafficking, arresting traffickers, and protecting victims. The Department also provides immigration relief to victims of human trafficking. The Blue Campaign is the unified voice for the DHS' efforts to combat human trafficking. Working in collaboration with law enforcement, government, non-governmental, and private organizations, the Blue Campaign strives to promote the basic right of freedom so that those who exploit human lives can be brought to justice. Increased awareness and training will lead to more tips to law enforcement, which will result in more victims being identified. To join in the DHS fight to end human trafficking, visit the Blue Campaign website at https://www.dhs.gov/blue-campaign or contact BlueCampaign@hq.dhs.gov to learn about available training, outreach materials, and victim assistance.

You can report tips to the ICE Tip line at 866-DHS-2-ICE, or 866-347-2423.

Specific Blue Campaign training products include:

- Web-based training about the indicators of human trafficking;
- Roll call videos explaining how available immigration relief for foreign victims provides a benefit to law enforcement;
- Scenario-based videos depicting indicators of sex trafficking and labor trafficking;
- Printed educational and reference materials for law enforcement and other first responders, non-governmental organizations, judicial officials, school staff, and victims or potential victims; and
- Human trafficking awareness posters and public service announcements.

To access these and other products, visit https://www.dhs.gov/blue-campaign.

DHS Common Operating Picture (COP) provides government and private sector Homeland Security Enterprise professionals with enhanced situational awareness, facilitating timely decision support prior to or in the aftermath of a natural disaster, act of terrorism, or man-made disaster. The DHS COP architecture, coupled with data from Homeland Security partners and Homeland Security Information Network (HSIN), provides actionable information, enhanced contextual understanding, and geospatial awareness. This enables government and private sector leaders to make timely and informed decisions, and to identify courses of action during an event or threat situation. The DHS COP provides users with a broad set of capabilities based on best-in-class technologies that deliver a rich, end user experience through a web-accessible interface. Access through the link to the DHS COP is on the top right side of the HSIN home page.

Homeland Security Information Network (HSIN) is a national, secure, and trusted web-based portal for information sharing and collaboration between federal, state, local, tribal, territorial, private sector, and international partners engaged in the homeland security mission. Using a single login credential, HSIN provides secure access from multiple networks, such as LEEP, RISSnet, Intelink, and TRIP*wire*. HSIN is made up of a growing network of communities, called Communities of Interest (COI). COIs are organized by state organizations, federal organizations, or mission areas, such as emergency management, law enforcement, critical sectors, and intelligence. Users can securely share within their communities or reach out to other communities as needed. HSIN provides secure, real-time collaboration tools, including a virtual meeting space, instant messaging, and document sharing. HSIN allows partners to work together instantly, regardless of their location, communicate, collaborate, and coordinate. This enables government and private sector leaders to make timely and informed decisions, and identify courses of action during an event or threat situation. For more information, visit https://www.dhs.gov/HSIN.

"If You See Something, Say Something™". The nationwide "If You See Something, Say Something™" public awareness campaign is a simple and effective program to raise public awareness of indicators of terrorism and terrorism-related crime, and to emphasize the importance of reporting suspicious activity to the proper local law enforcement authorities. The campaign was originally used by the New York Metropolitan Transportation Authority, which has licensed the use of the slogan to DHS for anti-terrorism and anti-terrorism crime-related efforts. For more information about the initiative, visit https://www.dhs.gov/see-something-say-something. To become an official partner and receive campaign materials, email seesay@hq.dhs.gov.

National Operations Center (NOC). In accordance with 6 U.S.C. 321(d), the National Operations Center serves as the principal operations center for the Department and shall:

- Provide situational awareness and a Common Operating Picture for the entire Federal Government; for State, local, tribal, and territorial governments; the private sector; and international partners; as appropriate; for events, threats, and incidents involving natural disasters, acts of terrorism, or other man-made disasters;
- Ensure that critical terrorism and disaster-related information reaches government decision-makers; and
- Enter into agreements with other Federal operations centers and other homeland security partners, as appropriate, to facilitate the sharing of information.

As defined by law, the term situational awareness means information gathered from a variety of sources that, when communicated to emergency managers and decision makers, can form the basis for incident management decision making.

National Terrorism Advisory System (NTAS) has replaced the Homeland Security Advisory System as the nation's primary domestic terrorism alerting resource. This system more effectively communicates information about terrorist threats by providing timely, detailed information to the public, government agencies, first responders, airports and other transportation hubs, and the private sector. It recognizes that Americans all share responsibility for the nation's security, and should always be aware of the heightened risk of terrorist attack in the U.S. and what they should do. After reviewing the available information, the Secretary of Homeland Security will decide, in coordination with other federal entities, whether an NTAS Alert should be issued. For more information, visit https://www.dhs.gov/national-terrorism-advisory-system.

U.S. Citizenship and Immigration Services (USCIS)

USCIS is the government agency that oversees lawful immigration to the United States. USCIS helps provide accurate information to a full range of stakeholders, including state and local agencies and applicants seeking immigration benefits. The agency is committed to ensuring the integrity of the nation's immigration system. Read the full mission statement at https://www.uscis.gov/aboutus.

Avoid Scams is a webpage for the public to learn how to recognize and report immigration scams and the unauthorized practice of immigration law, and to find authorized help with immigration services. To learn more, visit https://www.uscis.gov/avoid-scams, or https://www.uscis.gov/es/evitee stafas in Spanish.

Fraud Detection and National Security Directorate (FDNS). FDNS is embedded within USCIS offices across the country, and is staffed with immigration officers who are well-versed in immigration-related fraud, national security, and public safety issues. FDNS Immigration Officers not only provide support to adjudicators of immigration benefit applications, but also support programs sponsored by law enforcement agencies, such as Joint Terrorism Task Forces (JTTFs), Document and Benefit Fraud Task Forces (DBFTFs), and state and local fusion centers. Immigration officers' participation in these programs may be full-time, part-time, or virtual support. Immigration officers conduct administrative site visits and provide general or case-specific immigration information to law enforcement agencies under DHS guidance. Currently, there are more than 80 FDNS immigration officers in the JTTF Program and over 30 FDNS immigration officers in most of the 27 ICE-led DBFTFs. In addition, designated FDNS immigration officers in all 26 District Offices have made positive contact with a point-of-contact at state and local fusion centers. For more information, please contact USCISFODFDNSOps@uscis.dhs.gov.

Law Enforcement Support Operation Unit. USCIS's FDNS Directorate has developed a centralized operation to administer the S-Visa Program and facilitate the issuance of notional ("cover") immigration documents. The S Visa Program is available for aliens who possess "critical reliable information concerning a criminal organization or enterprise," and who are willing to share or have shared their information with a U.S. law enforcement agency or court and whose presence in the U.S. is necessary for the successful prosecution of criminal activity. The S-6 visa is available to aliens possessing "critical reliable information" regarding terrorist activity. State and federal law enforcement authorities (including federal or state courts and U.S. attorneys) can initiate a request under the "S" category. Requests for "S" status are processed through the requesting agency, the Department of Justice, and ultimately USCIS FDNS.

Notional immigration documents are genuine immigration documents issued to individuals who do not possess the associated immigration status. These documents are issued in furtherance of law enforcement investigations in order to create the appearance that an individual possesses or has been approved for a particular immigration status. Law enforcement requests for notional documents are submitted to U.S. Immigration and Customs Enforcement (ICE), which reviews the notional document request to ensure that documents are being requested for a legitimate investigative purpose. If ICE believes the document request is appropriate, USCIS will consider production of the requested document. For more information, visit https://www.uscis.gov/green-card/other-ways-get-green-card/green-card-informant-s-nonimmigrant.

USCIS' Public Engagement Division (PED) seeks to focus

on open, candid, and constructive collaboration with community stakeholders at all levels. PED is dedicated to coordinating and directing agency-wide dialogue with external stakeholders to actively collaborate and maintain open and transparent communication and to seek feedback regarding policies, priorities, and organizational performance reviews. For more information, visit https://www.uscis.gov/outrreach or contact Public.Engagement@uscis.dhs.gov.

USCIS Resources is a webpage with links to a variety of publications and other materials for individuals seeking immigration benefits, the organizations that serve them, and the public. For more information, visit http://www.uscis.gov/resources. USCIS provides the latest version of its applications and petitions on its website. All forms are free and available at https://www.uscis.gov/forms. For more information, contact Public.Engagement@dhs.gov.

T and U Nonimmigrant Status ("T Visas" and "U Visas") for Victims of Human Trafficking and Other Qualifying Crimes. The T visa is generally available for victims of human trafficking who have complied with any reasonable request for assistance in the investigation or prosecution of the human trafficking, and who meet other requirements. The U visa is generally available for victims of certain qualifying crimes who have been, are being, or are likely to be helpful to law enforcement in the investigation or prosecution of the crime, and who meet other requirements. Federal, state, local, tribal, or territorial law enforcement agencies may sign a law enforcement certification for the victim detailing the crime and the victim's cooperation in the investigation or prosecution. U visa petitioners are required to submit this law enforcement certification with their petitition. T visa applicants may submit a law enforcement certification with their petition. Law Enforcement Agencies are never required to sign a certification, and are not responsible for determining eligibility for a T or U visa. The victim applies to USCIS for a T or U visa, and USCIS reviews the application and all submitted evidence, including any law enforcement certifications, to determine eligibility. Related resources include:

- **The U and T Visa Law Enforcement Resource Guide** provides law enforcement officials information about T and U visa requirements, the law enforcement certification process, and answers to frequently asked questions from law enforcement agencies to support investigations and prosecutions involving victims of human trafficking and other crimes. The guide is available at https://www.dhs.gov/publication/u-visa-law-enforcement-certification-resource-guide.

- **Information for Law Enforcement Agencies and Judges**. USCIS has a webpage for law enforcement agencies and judges that explains the different types of benefits available for victims of human trafficking and other crimes. It also describes procedures for law enforcement, including a list of "Important Things to Remember". Other materials include roll call videos, information about continued presence (a temporary immigration status administered by ICE for victims of human trafficking), and links to the T visa declaration form and U visa certification form. Both of these forms are completed by the investigating or prosecuting agency but submitted to USCIS by the victim. For more information, visit https://www.uscis.gov/tools/resources/information-law-enforcement-agencies-and-judges. For law enforcement inquiries, contact LawEnforcement_UTVAWA.vsc@uscis.dhs.gov.

- **In-Person and Web-Based Training**. USCIS offers in-

person and web-based presentations for law enforcement on T and U visas. If interested, please contact USCIS at T_U_VAWATraining@uscis.dhs.gov.

Office of the Citizenship and Immigration Services Ombudsman (CIS Ombudsman)

The CIS Ombudsman is available to help law enforcement with issues or concerns they have regarding their interactions with USCIS. The CIS Ombudsman is an independent, impartial, and confidential office within DHS Headquarters that helps individuals and employers resolve problems with USCIS applications and petitions. The office also makes recommendations to fix systemic problems and improve the overall delivery of services provided by USCIS.

Send Your Recommendations to the CIS Ombudsman. The CIS Ombudsman is dedicated to identifying systemic issues in the immigration benefits process and preparing recommendations for submission to USCIS for process changes. Send examples of identified issues and suggestions to cisombudsman@hq.dhs.gov.

Submit a Request for Case Assistance to the CIS Ombudsman. If you, or someone you are working with, are experiencing problems during the adjudication of an immigration benefit with USCIS, you can submit an electronic DHS Form 7001 through the Ombudsman Online Case Assistance system. To submit a request for assistance on behalf of another, follow the form instructions to ensure the appropriate party consents to your submission. For more information, visit https://www.dhs.gov/case-assistance.

Office for Civil Rights and Civil Liberties (CRCL)

DHS CRCL is available to help law enforcement with issues relating to the DHS mission and the protection of civil rights and civil liberties. CRCL works with other DHS offices and components to develop policies, programs, and training material. It also investigates complaints alleging violation of rights, programs, or policies by DHS employees, leading to recommendations to fix identified problems and help DHS safeguard the Nation, while preserving individual liberty, fairness, and equality under the law.

CRCL is also responsible for assuring that the Department's federally-assisted programs comply with various civil rights laws, including, but not limited to, Title VI of the Civil Rights Act of 1964, as amended; Title IX of the Education Amendments of 1972, as amended; Section 504 and the Rehabilitation Act of 1973, as amended; Age Discrimination Act of 1975, as amended (Age Act); and DHS regulation 6 C.F.R. Part 19, Nondiscrimination in Matters Pertaining to Faith-based Organizations.

Civil Rights Requirements in Federally-Assisted Programs. CRCL provides resources, guidance, and technical assistance to recipients of DHS financial assistance on complying with Title VI of the Civil Rights Act of 1964 (Title VI); Section 504 of the Rehabilitation Act of 1973; 6 C.F.R., part 19; and related requirements. Information for recipients on meeting their nondiscrimination requirements under Title VI is available on CRCL's website, https://www.dhs.gov/publication/title-vi-dhs.

DHS also published guidance to help those who carry out Department-supported activities to understand and implement their obligations under Title VI to provide meaningful access for people with limited English proficiency (https://www.dhs.gov/guidance-published-help-department-supported-organizations-provide-meaningful-access-people-limited). For more information, contact crcl@hq.dhs.gov.

Common Muslim American Head Coverings and Common Sikh American Head Coverings Posters. CRCL provides guidance to Department personnel on the appropriate ways in which to screen and, if necessary, search Muslim or Sikh individuals wearing various types of religious head coverings. Although these posters are primarily designed for DHS personnel, they are available to state and local law enforcement. For more information, visit www.dhs.gov/civil-rights-and-civil-liberties-institute.

Educational posters in customizable digital and hard copy form can be ordered from the DHS CRCL by emailing crcltraining@hq.dhs.gov.

Community Roundtables. CRCL leads, or plays a significant role in, regular roundtable meetings across the country in over 15 U.S. cities. These roundtables bring exceptionally diverse demographic communities together with federal, state, local, tribal, and territorial government representatives. Issues discussed range from immigration and border issues to civil rights issues in aviation security. CRCL also conducts roundtables with young leaders of diverse communities. For more information, contact communityengagement@hq.dhs.gov.

Countering Violent Extremism (CVE) Training Guidance and Best Practices. This written guidance provides best practices for federal, state, and local government and law enforcement officials organizing CVE, cultural awareness, and counterterrorism training. For more information, visit https://www.dhs.gov/civil-rights-and-civil-liberties-institute.

DHS Complaint Avenues Guide. DHS has many avenues for the public to make complaints involving DHS employees or programs, alleged violations of civil rights and civil liberties, immigration filing, travel redress, and other types of grievances. CRCL developed a guide that brings together information about these avenues. For more information, visit http://www.dhs.gov/sites/default/files/publications/dhs-complaint-avenues-guide_10-03-12_0.pdf.

The CRCL Newsletter is distributed monthly to inform stakeholders and the public about office activities, including how to make complaints; ongoing and upcoming projects; and opportunities to offer comments and feedback. Newsletters are distributed via an email list to thousands of non-governmental organizations, community members, and government partners, and made available to community groups for redistribution. For more information, visit https://www.dhs.gov/publication/crcl-newsletter.

How to File and Submit a Complaint. Under 6 U.S.C. § 345 and 42 U.S.C. § 2000ee-1, CRCL reviews and assesses information concerning abuses of civil rights, civil liberties, and profiling on the basis of race, ethnicity, or religion, by employees and officials of DHS. Complaints are accepted in languages other than English. For more information, visit https://www.dhs.gov/file-civil-rights-complaint or email directly to CRCLCompliance@hq.dhs.gov.

"I Speak" Language Identification Pocket Guides and Posters. CRCL has created a set of three tools ("I Speak" poster, pocket guide, and job aid) for use by state and local law enforcement officers who work directly with the public, and who may need to identify the language of the person with whom they are interacting. These tools support the Language Access Plans that many sheriffs' offices have put in place to meet the requirements of Title VI of the Civil Rights Act of 1964, as amended. The "I Speak" format includes 75 of the most frequently encountered languages, as well as 13 of the indigenous languages of Mexico and Central America. For more information, digital copies, or samples, email crcltraining@hq.dhs.gov.

Law Enforcement Awareness Brief (LAB) on Terrorism Prevention. The LAB is a customizable brief designed for small and mid-sized state, local, and tribal law enforcement agencies that focuses on their role in the national terrorism prevention strategy. The LAB is a central element of a broader DHS Training-of-Trainers (ToT) program developed to support a national cadre of state, local, and tribal law enforcement instructors who, after completing the DHS ToT program, will offer the brief in their home jurisdictions to other law enforcement personnel. For more information, email crcltraining@hq.dhs.gov.

Privacy, Civil Rights and Civil Liberties Fusion Center Training Program. The Implementing Recommendations of the 9/11 Commission Act require that DHS support fusion centers by providing training on privacy, civil rights, and civil liberties. As a result, CRCL and the DHS Privacy Office have partnered with the DHS Office of Intelligence and Analysis and the U.S. Department of Justice Bureau of Justice Assistance to deliver this training program. The program has included: A website resource center https://www.it.ojp.gov/PrivacyLiberty; a training of Privacy/Civil Liberties Officers program; a technical assistance program; and an on-site training program. Topics covered include: civil rights and civil liberties basics and "red flags" (how to spot potential issues and incorporate safeguards into procedures); privacy fundamentals (how to integrate privacy policy and recognize and respond to a privacy incident); cultural tactics for intelligence and law enforcement professionals (covers frequently encountered misconceptions and stereotypes and addresses policies against racial or ethnic profiling); and First Amendment issues in the information sharing environment (covers considerations when fusion centers may encounter constitutionally protected activities, such as freedom of speech, demonstrations, petitions for redress, etc.). Fusion centers and their liaison officer networks have the option of choosing additional topics to create a customized agenda. For more information, email FusionCenterTraining@hq.dhs.gov.

Note on Current Status: While this program does not currently provide on-site training due to lack of funding, extensive materials and technical assistance are available.

Web Portal for Privacy and Civil Rights and Civil Liberties Officers. This portal provides training materials and video resources for state and local personnel and trainers on privacy, civil rights, and civil liberties issues encountered by fusion centers and justice entities. The recently updated web portal includes over 30 pages of new content specifically geared toward privacy and civil rights and civil liberties officers. The portal was developed as a result of a partnership between CRCL, Privacy Officers, and the DHS Office of Intelligence and Analysis. This is available at: https://www.it.ojp.gov/PrivacyLiberty.

United States Coast Guard (USCG)

USCG has a wide array of surface, air, and specialized assets and capabilities available for multiple levels of response, patrol, and mission specific tasks.

Surface platforms consist of boats and cutters. Vessels under 65 feet in length are classified as boats and usually operate near shore, on inland waterways, and from cutters. Craft include: Motor Lifeboats; Medium and Small Response Boats; special purpose response boats; port security boats; Aids to Navigation boats; and a variety of smaller, non-standard boats including rigid hull inflatable boats. Sizes range from 64-foot in length down to 12-foot. Cutters are commissioned USCG vessels 65 feet in length or greater, having adequate accommodations for crew to live onboard. Cutters usually have one or more rigid hull inflatable boats onboard. Polar Class icebreakers also carry an Arctic Survey Boat and Landing

Craft. The USCG cutter fleet ranges from a 420-foot Icebreaker to a 65-foot harbor tug; however, the most commonly recognized and widely utilized are National Security Cutters, High and Medium Endurance Cutters (418-foot, 378-foot, 270-foot, and 210-foot) and smaller 87-foot Marine Protector Class, 110-foot Island Class, and 154-foot Sentinel Class patrol vessels.

There are a total of 203 aircraft in Coast Guard inventory, a figure that will fluctuate due to operational and maintenance schedules. Major Missions consist of Search/Rescue, Law Enforcement, Environmental Response, Ice Operations, and Air Interdiction. Fixed-wing aircraft (C-130 Hercules, C-27 Spartan, C-144 Ocean Sentry, and C-37 Gulfstream) operate from large and small Air Stations. Rotary wing aircraft (H-65 Dolphin and H-60 Jayhawk helicopters) operate from flight-deck equipped Cutters, Air Stations, and Air Facilities.

USCG Deployable Specialized Forces (DSF) provides additional teams and resources such as Maritime Safety and Security Teams (10), Port Security Units (8), Tactical Law Enforcement Teams (2), Maritime Security Response Team (2), National Strike Force and Regional Dive Lockers (3). DSF teams are capable of worldwide deployment via air, ground, or sea transportation in response to changing threat conditions and evolving Maritime Homeland Security mission requirements. Core capabilities include: Enhanced Law Enforcement Boarding; Waterside Security/Force Protection; Landside Security/Force Protection; Port Security; Subsurface Operations; Chemical, Biological, Radiological, Nuclear and Enhanced Conventional Weapons (CBRNE) Detection and Identification; Disaster Response; Environmental Response; Deployable Incident Management; Advanced Planning; and multiple supporting capabilities.

America's Waterways Watch is a combined effort of the USCG and its Reserve and Auxiliary components to enlist the active participation of those who live, work, or play around America's waterfront areas. For more information, contact aww@uscg.mil or visit http://americaswaterwaywatch.uscg.mil. To report suspicious activity call 877-24WATCH (877-249-2824).

USCG Maritime Information Exchange ("CGMIX") makes USCG maritime information available to the public on the Internet in the form of searchable databases. Much of the information on the CGMIX website comes from the USCG's Marine Information for Safety and Law Enforcement (MISLE) information system. For more information, visit http://cgmix.uscg.mil/.

USCG Navigation Center supports safe and efficient maritime transportation by delivering accurate and timely maritime information services and Global Positioning System (GPS) augmentation signals that permit high-precision positioning and navigation. For more information, visit https://www.navcen.uscg.gov/ or call 703-313-5900.

USCG Sector Command Centers. Given USCG mission diversity, asset readiness status and ongoing operations, the main avenue for proper and expeditious USCG asset mobilization requests are through USCG Sector Command Centers. There are 37 USCG Sectors.

Commands throughout the U.S. and U.S. territories:

Sector Command Centers

Sector Name	Locations	24/7 Contact
Anchorage	Anchorage, AK	907-428-4100
Maryland NCR	Baltimore, MD	410-576-2693
Boston	Boston, MA	617-223-5757
Buffalo	Buffalo, NY	716-843-9527
Charleston	Charleston, SC	843-740-7050
Columbia River	Warrenton, OR	503-861-6211
Corpus Christi	Corpus Christi, TX	361-939-6393
Delaware Bay	Philadelphia, PA	215-271-4940
Detroit	Detroit, MI	313-568-9560
Guam	Santa Rita, Guam	671-355-4824
Hampton Roads	Portsmouth, VA	757-668-5555
Honolulu	Honolulu, HI	808-842-2600
Houston-Galveston	Houston, TX	281-464-4854
Humboldt Bay	McKinleyville, CA	707-839-6123
Jacksonville	Atlantic Beach, FL	904-714-7558
Juneau	Juneau, AK	907-463-2980
Key West	Key West, FL	305-292-8727
Lake Michigan	Milwaukee, WI	414-747-7182
LA-Long Beach	San Pedro, CA	310-521-3600
Lower Mississippi	Memphis, TN	901-521-4822
Long Island	New Haven, CT	800-774-8724
Miami	Miami Beach, FL	305-535-4472
Mobile	Mobile, AL	251-441-5720
New Orleans	New Orleans, LA	800-874-2153

New York	Staten Island, NY	718-354-4120
North Bend	North Bend, OR	541-756-9220
North Carolina	Wilmington, NC	910-343-3880
Northern New England	South Portland, ME	207-767-0303
Ohio Valley	Louisville, KY	502-779-5400
Puget Sound	Seattle, WA	206-217-6001
San Diego	San Diego, CA	619-278-7000
San Francisco	San Francisco, CA	415-399-3530
San Juan	San Juan, PR	787-289-2041 787-729-6770
Sault Ste. Marie	Sault Ste. Marie, MI	906-635-3230
Southeastern New England	Woods Hole, MA	508-457-3211
St. Petersburg	St. Petersburg, FL	727-824-7506
Upper Mississippi	St. Louis, MO	314-269-2500

Office of Terrorism Prevention Partnerships (OTPP)

The Office of Terrorism Prevention Partnerships (OTPP), formerly named the Office for Community Partnerships (OCP), continues to lead, facilitate, and oversee DHS terrorism prevention programs. OTPP is responsible for catalyzing and supporting the requirements of state, local, tribal, territorial, and non-governmental, community-based efforts to implement prevention programs within the United States that target radicalization and mobilization to violence for all forms of terrorism.

OTPP enhances education and community awareness regarding the threat, provides resources to support terrorism prevention stakeholders where applicable, coordinates relevant DHS terrorism prevention activities, actively counters terrorist radicalization and recruitment, and promotes early warning so that frontline defenders can intervene to stop attacks and help prevent individuals from going down the path to violence.

Enhanced Engagement and Training Resources.
For DHS, terrorism prevention must render terrorism ineffective as a tactic in the United States by diminishing opportunities for recruitment and inspiration for the support and use of ideologically motivated violence. It is a critical DHS mission, and OTPP is acting to meet the rising and ever changing threat of terrorist recruitment and inspiration to violence in the United States. By sharing the most up-to-date information on organizations and operational tactics, as well as some of the case studies OTPP has seen throughout the United States, OTPP can unveil some of the mystery around violent extremism, and subsequently arm partners with the information needed to intervene, foster resilience in communities, and even prevent violent extremist recruitment.

The Community Awareness Briefing (CAB)
OTPP has improved and expanded outreach to diverse communities, increased awareness about radicalization to violence, attended cultural events, and hosted dozens of international visitors to share work and learn new ideas. Local organizations are best positioned to address people at risk for radicalization and mobilization to violence. To enhance engagement efforts and provide awareness training in regards to terrorism prevention, DHS, in partnership with the National Counterterrorism Center (NCTC), participated in recent updates of the Community Awareness Briefing (CAB) to expand the domestic terrorism content it delivers, and has supported its delivery across the country to communities and state, local, and federal law enforcement.

The Law Enforcement Awareness Briefing (LAB)
DHS also has supported the in-house development of a Law Enforcement Awareness Briefing (LAB) to provide law enforcement officers, especially those in small to medium-sized agencies at the state, local, tribal, and territorial levels, with the latest information on terrorism prevention trends and efforts. It focuses on the unique roles and issues that law enforcement officers face when they deal with issues relating to terrorism prevention. This briefing is in its final stages of pilot testing and review, and it should be available for wide distribution to law enforcement officers in 2018.

Moreover, OTPP also continues to work alongside its 26 Countering Violent Extremism (CVE) grantees, whose period of performance began August 1, 2017. The CVE Grant Program (CVEGP) was appropriated by Congress to state and local

governments, universities, and non-profit organizations in order to assist local communities in their own efforts to counter violent extremism. The grants are structured around five focus areas: developing community resilience to violent extremism recruitment; training for, and engagement with, local partners tackling the challenge of violent extremism; support for programs that intervene in the radicalization process to "off-ramp" potentially radicalized individuals; challenging extremists' narratives; and building the capacity of local partners to sustainably address issues related to violent extremism. More information about the CVEGPis available at https://www.dhs.gov/cvegrants

To learn more about terrorism prevention initiatives, please email TerrorismPrevention@hq.dhs.gov, or visit https://www.dhs.gov/countering-violent-extremism#.

U.S. Customs and Border Protection (CBP)

CBP is one of the DHS' largest and most complex components, with a priority mission of keeping terrorists and their weapons out of the United States. It also has a responsibility for securing the border and facilitating lawful international trade and travel, while enforcing hundreds of U.S. laws and regulations, including immigration and customs laws. For more information, visit www.cbp.gov or contact 202-344-1700.

The **Carrier Liaison Program** provides standardized training and assistance to international air carriers related to admissibility and fraudulent document detection in order to encourage carrier compliance with U.S. immigration laws. For more information about the Carrier Liaison Program, visit www.cbp.gov/travel/travel-industry-personnel/carrier-liaison-prog or contact CLP@dhs.gov or 202-621-7817.

CBP Border Community Liaison Program. Border Community Liaisons focus on outreach to community stakeholders and provide fact-based information regarding the CBP mission, functions, authorities, and responsibilities. For more information about Border Community Liaisons nationwide please email Maria E. Ibanez at Maria.E.Ibanez@cbp.dhs.gov.

The **CBP Information Center (CIC)** serves as the primary CBP liaison to the general public, enabling legitimate trade and travel by providing accurate and timely information regarding CBP regulations, processes, procedures, and trusted traveler programs. The CIC also serves as the conduit for the public to ask questions or submit compliments and complaints regarding the agency. The CIC can be reached at 877-CBP-5511 or 202-325-8000.

CBP Laboratories and Scientific Services coordinates technical and scientific support to all CBP and DHS-wide trade and border protection activities including laboratory analysis for trade enforcement and product safety, forensic services for criminal investigations, and 24/7 telephonic access to scientific resources for technical case adjudication for radiation/nuclear materials and other potential weapons of mass effect. For more information, visit https://www.cbp.gov/about/labs-scientific-svcs.

Intellectual Property Rights (IPR) Help Desk. CBP's IPR Help Desk provides information on IPR border enforcement procedures and receives allegations of IPR infringement. Questions regarding IPR enforcement at U.S. borders and information on IPR infringing goods that may be entering the U.S. can be directed to the IPR Help Desk at 562-980-3119 ext. 252, or via email at jpr.helpdesk@dhs.gov.

Missing or Late International Travelers. Information regarding reported missing or late international travelers can be obtained from the nearest port of entry. For a list of ports, visit https://www.cbp.gov/contact/ports.

Intergovernmental Public Liaison (IPL). The Intergovernmental and Public Liaison is CBP's liaison to state, local, tribal, and territorial governments and non-governmental organizations. IPL facilitates communication between the agency and these stakeholders regarding CBP initiatives and policies.

IPL serves the dual role of representing the intergovernmental and external perspective in the federal policymaking process, as well as clarifying the federal perspective to intergovernmental officials and external stakeholders. IPL aims to enhance communication and partnerships with local, state, tribal, and territorial governments, as well as the general public, and a variety of external partners, such as academia, private sector and not-for profit groups, and national organizations. Questions for IPL can be directed to CBP-INTERGOVERNMENTAL-PUBLIC-LIAISON@cbp.dhs.gov or 202-325-0775.

No Te Engañes (Don't be Fooled) is the CBP outreach campaign to raise awareness of human trafficking among potential migrants. For more information, visit https://www.cbp.gov/border-security/human-trafficking/no-te-enganes or contact Laurel Smith at laurel.smith@dhs.gov or 202-344-1582.

Port of Entry Information. CBP enforces the import and export laws and regulations of the U.S. Federal Government, processes international passengers and cargo, and performs agriculture inspections at ports of entry. Port personnel are the face at the border for most cargo and persons entering the United States. For a list of ports, visit https://www.cbp.gov/contact/ports.

Preventing International Non-Custodial Parental Child Abduction. CBP partners with the Department of State's (DOS) Office of Children's Issues to prevent the international abduction of children involved in custody disputes or otherwise against the published order of the court. Concerns about the international travel of a child, can be addressed to the DOS Office of Children's Issues at PreventAbduction@state.gov or the 24 hour hotline 888-407-4747.

Suspicious Aircraft or Boats. The CBP Air and Marine Operations Center (AMOC) is responsible for securing the airspace at and beyond the Nation's borders through detection, monitoring, sorting, and interdiction of general aviation and maritime threats. Suspicious air or maritime activity, to include low flying aircraft and drug or human smuggling activity, should be directed to AMOC at 1-866-AIRBUST.

Tip Line. Suspicious activity regarding international travel and trade can be reported to CBP at 1-800-BE-ALERT.

Visa Waiver Program (VWP) enables citizens and nationals from 38 countries to travel to and enter the U.S. for business or visitor purposes for up to 90 days without obtaining a visa. For more information about the Visa Waiver Program, visit http://www.cbp.gov/travel/international-visitors/visa-waiver-program.

Countering Weapons of Mass Destruction (CWMD)

The CWMD Office supports operational partners in their preventing, detecting, and responding to WMD terrorism against the United States, and it promotes readiness for chemical, biological, radiological, nuclear, and other health security threats. The CWMD Office is composed chiefly of the Domestic Nuclear Detection Office (DNDO) and the Office of Health Affairs (OHA).

The CWMD Office, through the Chief Medical Officer, serves as the DHS point of contact on medical and public health issues related to natural disasters, acts of terrorism, and other man-made disasters for federal departments and agencies; state,

local, tribal, and territorial (FSLTT) governments; the medical community; and the private sector.

The health, safety, and readiness of the DHS workforce are key enablers of mission success. The presence of these factors is vital to the integrity of operational capability, reliability, continuity, and mission accomplishment; the absence of these factors can have significant national security implications. Recognizing the salience of these points, the DHS reorganization that combined DNDO with OHA to form CWMD in December 2017 included a functional alignment of OHA assets from the Workforce Health and Medical Support Division to the Office of the Chief Human Capital Officer (OCHCO), within the domain of the Under Secretary for Management (USM). This functional alignment provides the Department with leverage to guide DHS towards an integrated health, safety, and readiness culture.

Countering Weapons of Mass Destruction (CWMD) Operations, located within the Department of Homeland Security's National Operations Center (NOC), provides Chemical, Biological, Radiological, and Nuclear (CBRN) situational awareness and information sharing related to CBRN incidents by:

- Providing a Common Operating Picture for the Department of Homeland Security, FSLTT partners, the private sector, and international partners in coordination with the Departments of State, Defense, Justice, and Energy, as appropriate, related to CBRN events, threats, or incidents involving natural disasters, acts of terrorism, or other man-made disasters.
- Ensuring that critical CBRN incident and disaster-related information reaches government decision-makers.
- Collaborating with Department of Homeland Security and other Federal operations centers to facilitate the sharing of information.

Contact information: 877-363-6522 or e-mail CWMD.NOC@hq.dhs.gov, 866-789-8304 or e-mail CWMD.NOC@hq.dhs.gov.

The **Data Mining, Analysis, and Modeling Cell** (DMAMC) is a team of subject matter experts from the radiation detection community responsible for leveraging existing data and analysis methods to answer scientific and technical questions posed by CWMD stakeholders related to the radiological detection mission. For more information contact the DMAMC at DMAMC1@hq.dhs.gov.

Radiological and Nuclear Detection Community of Interest (COI). CWMD's R/N Detection COI is a site located on the Homeland Security Information Network that provides a repository CWMD, R/N detection, and other nuclear detection related activities that can be accessed by external users. It is also a forum where nuclear detection community stakeholders can securely collaborate and share best practices and lessons learned. State, local, tribal, and territorial law enforcement, fire, emergency management and radiation health personnel, federal agencies, federally-funded research and development centers, and academia directly supporting nuclear detection capability development at all levels of government are encouraged to join the site with other GNDA community stakeholders. To join the R/N Detection COI, submit a request by email to CWMD with a message subject line of: "CWMD PRND COI HSIN Access Request" to the address: PRND_COI@hq.dhs.gov.

Equipment Test Results. CWMD equipment test campaigns evaluate the effectiveness of detection systems such as: radiation isotope identification devices (RIIDs), personal radiation

detectors (PRDs), backpacks, and mobile systems (vehicle-mounted, boat-mounted, and aerial-mounted).

FSLTT partners intending to purchase radiological/nuclear (R/N) detection equipment are strongly encouraged to consider instruments that have been independently tested by accredited laboratories and have demonstrated conformity with the applicable American National Standards Institute/ Institute of Electrical and Electronics Engineers (ANSI/IEEE) N42 standards. Manufacturers offering new equipment for consideration should be asked to provide evidence of independent testing for compliance with these standards. CWMD has resources that are available to inform and assist FSLTT partners when selecting the right R/N detection equipment to meet their operational needs.

Reports and additional analyses may be obtained through DMAMC; requests should be sent to DMAMC1@hq.dhs.gov.

Open Access to American National Standards Institute (ANSI) N42 Series Standards. CWMD sponsors the IEEE's providing copies of the ANSI N42 Radiation Detection Standards free of charge to anyone who wants a copy. The website to obtain the latest published version of one of the sponsored standards is http://standards.ieee.org/about/get/.

The GRaDER® Program. GRaDER® provides objective and reliable performance testing information to FSLTT stakeholders for R/N detection equipment tested against consensus and technical capability standards to assist in making informed R/N detection equipment procurements. For more information, visit https://www.dhs.gov/guidance-grader-program or email GRaDER.questions@hq.dhs.gov.

Mobile Detection Deployment Units (MDDU). MDDUs are mobile trailer packages containing radiation detection equipment for up to 40 public safety professionals. MDDU packages are deployed across the United States. The equipment includes PRDs, portable backpack radiation detection units, high and low-resolution radiation identification hand-held instruments, mobile radiation detection systems, and interoperable communications and tracking equipment. Each MDDU is accompanied by technical support staff to train FSLTT personnel on the use of the specific MDDU equipment, and to help integrate these capabilities into existing operations.

Collaboration between FSLTT law enforcement and public safety agencies is crucial to a layered approach to radiological and nuclear security. CWMD developed the MDDU as a surge asset to support FSLTT partners' detection and reporting of radiological and nuclear threats. The MDDU is designed to supplement radiological and nuclear detection capabilities in support of national special security events (NSSEs) or in response to an intelligence-driven event with Federal law enforcement integration.

Federal, state, local, tribal, and territorial agencies may request an MDDU by contacting CWMD at DNDO_MDDU_Request@hq.dhs.gov.

WMD Detection Exercises. CWMD's Exercise Program provides support to FSLTT partners in developing, designing, and conducting discussion or operational-based CBRN detection exercises that are compliant with the Homeland Security Exercise and Evaluation Program methodology, at no cost to stakeholders. Exercises provide valuable hands-on experience for FSLTT personnel performing WMD detection missions and assist decision makers in integrating the detection mission into their daily operations. Additional information about WMD detection exercises is available by contacting CWMD at brady.ohanlon@hq.dhs.gov or sean.hearns@hq.dhs.gov.

Radiological and Nuclear Detection Training. CWMD's Training Program provides

quality products to support, develop, enhance, and expand R/N detection capabilities in support of the global detection architecture. Together with other federal partners, the CWMD Training Program provides instructional courses on R/N detection tactics, techniques, and procedures. The CWMD Training Program conducts technical review, evaluation, and continual developmental improvement of the R/N detection training curriculum. These reviews increase the operational detection capabilities of FSLTT partners to detect and interdict R/N materials and/or devices. The program seeks to develop and implement protocols and training standards for effective use of R/N detection equipment and the associated alarm reporting and resolution processes.

R/N detection training courses and curricula are available both online and in the classroom through CWMD and its partnered training providers. For more information e-mail DNDOTraining@hq.dhs.gov. Courses also are available through the FEMA Federal Sponsored Course catalog.

Securing the Cities (STC) Program. The STC program seeks to reduce the risk of a successful deployment of a radiological/nuclear (R/N) weapon against major metropolitan areas and the pathways leading to those areas to detect, analyze, and report nuclear and other radioactive materials out of regulatory control. STC cooperative agreement implementations include New York and Jersey City/Newark, Los Angeles/Long Beach, the National Capital Region, Houston, and Chicago. In FY2018 CWMD intends to expand the scope of the STC Program to include a regional pathway approach in the development of detection capabilities. The pathway concept will concentrate on known smuggling routes, and put in place a regional detection capability that integrates FSLTT assets within a large geographic region. Initial pathway implementations will encompass the likely routes through the Caribbean and the Southwest border. CWMD will target R/N detection capabilities for select cities within each of these regions and also provide resources to the agencies that cover the transportation networks through these regions. For more information, email DNDOSTC@hq.dhs.gov.

BioWatch Program. BioWatch is a nationwide biosurveillance monitoring system operating in more than 30 metropolitan areas across the country that is designed to detect the release of select aerosolized biological agents. The Office of Health Affairs (OHA) within the CWMD Office provides program oversight for the BioWatch program, while state and local agencies operate the system in their jurisdictions. BioWatch is a collaborative effort of multidisciplinary partners at the federal, state, and local level, including public health, laboratory, environmental agencies, emergency management, and law enforcement. Jurisdictional preparedness and response planning efforts related to the BioWatch program are developed through these partnerships. BioWatch partnerships bring experts at every level of government together to enhance resilience.

The First Responder Guidance for Improving Survivability in Improvised Explosive Device (IED) and/or Active Shooter Incidents was developed at the request of the National Security Council's working group on IED situations, and in response to first responders who have encountered mass casualties from IEDs and/or active shooter incidents. Led by CWMD's Medical First Responder Coordination Branch, the guide was developed in coordination with the Departments of Defense, Health and Human Services, Justice, and Transportation. The Guide is available at https://www.dhs.gov/publication/iedactive-shooter-guidance-first-responders.

The National Biosurveillance Integration Center (NBIC) integrates and analyzes information about biological threats to human, animal, plant, and environmental health to

help ensure the Nation's responses are well-informed, save lives, and minimize economic impact. NBIC works in partnership with FSLTT and private sector partners to synthesize and analyze information collected from across the spectrum of these organizations to provide more rapid identification of and response to biological threats. NBIC shares this information with stakeholders via the DHS Common Operating Picture (COP), providing a comprehensive electronic picture with assessments of current biological events, trends, and their potential impacts on the Nation's homeland security. Additionally, access to state and local NBIC Biosurveillance Reports is available on the Homeland Security Information Network (HSIN) and through direct email distribution, by request, to public health, health care, agriculture, environment, and law enforcement personnel across the country at all levels of government. To request NBIC Reports via direct email distribution or to request access to HSIN-NBIC-SL, contact nbicoha@hq.dhs.gov.

Federal Emergency Management Agency (FEMA)

FEMA's mission is to support citizens and first responders to ensure the nation builds, sustains, and improves its capability to prepare for, protect against, respond to, recover from, and mitigate all hazards.

All-Hazards Emergency Planning Guides. In accordance with *Now is the Time: The President's Plan to Protect Our Children and Our Communities by Reducing Gun Violence*, FEMA along with other components of DHS, and the Departments of Health and Human Services, Justice, and Education, collaboratively designed and published revised all-hazards emergency management planning guides that include sections that address the importance of preparing for, preventing, protecting against, mitigating, responding to, and recovering from an active shooter or mass casualty incident. This joint federal effort has resulted in the development of three guides designed for Houses of Worship, Institutions of Higher Education, and Schools from Kindergarten through Twelfth Grade. For more information and electronic copies of the guides visit, https://www.fema.gov/plan.

The **Authorized Equipment List (AEL)** published and maintained by the FEMA Grant Programs Directorate (GPD), is a tool used by grant recipients to determine allowability of equipment types for FEMA's Preparedness Grant Programs. The AEL is used to facilitate more effective and efficient procurement of items under specific FEMA Preparedness Grants by informing grantees of relevant standards, operating considerations, and programmatic considerations associated with each equipment item. The AEL consists of 21 equipment categories, ranging from Personal Protective Equipment (PPE) to Medical Supplies to Terrorism Incident Prevention Equipment. The AEL exists with considerable overlap with the Standard Equipment List (SEL), a comprehensive list of first responder equipment maintained by the Interagency Board (IAB), an inter-governmental group with representation from multiple federal agencies and the first responder community, and strong connections to subject matter experts in all equipment areas. GPD works in close collaboration with the IAB on the items and relevant information that is maintained on the AEL. The AEL has an interactive version that allows grantees to search for items by keyword, equipment category, or item number. Each item page number includes a unique number identifier, the equipment title, the specific grant program(s) for which the item is allowable, a description of the item, and grant notes that specify policy requirements for use and purchase. For more information, visit https://www.fema.gov/authorized-equipment-list.

Comprehensive Preparedness Guide 502: Considerations for Fusion Center and Emergency Operations

Center Coordination provides state and major urban area fusion center and emergency operations center (EOC) officials with guidance for the coordination between fusion centers and EOCs. It outlines the roles of fusion centers and EOCs and provides steps by which these entities can work together to share information and intelligence on an ongoing basis. CPG 502 supports the implementation of the *Baseline Capabilities for State and Major Urban Area Fusion Centers*, and likewise, assists EOCs to fulfill their missions in both steady state and active state emergency operations. CPG 502 provides guidance on the broad capability requirements of an EOC. The guide is available at https://www.fema.gov/media-library/assets/documents/25970.

First Responder Training.

- Center for Domestic Preparedness (CDP), is DHS's only federally chartered Weapons of Mass Destruction (WMD) training center committed to having an emergency response community prepared for and capable of responding to all-hazards events. The interdisciplinary resident and nonresident training courses at CDP promote a greater understanding among these diverse responder disciplines:

Agricultural Safety, Citizen/Community Volunteer, Education, Emergency Management, Emergency Medical Services, Fire Service, Governmental Administrative, Hazardous Materials, Healthcare, Information Technology, Law Enforcement, Public Health, Public Safety Communications, Public Works, Search and Rescue, Security and Safety, and Transportation.

- Emergency Management Institute (EMI) serves as the national focal point for the development and delivery of emergency management training to enhance the capabilities of state, local, tribal, and territorial government officials; volunteer organizations; FEMA's disaster workforce; other federal agencies; and the public and private sectors to minimize the impact of disasters and emergencies on the American public. Visit EMI and access training through https://training.fema.gov/.

- National Training and Education Division/Training Partners Program (NTED/TPP) through the National Domestic Preparedness Consortium and Continuing Training Grants Partners serves the nation's first responder community, offering more than 170 courses to help build critical skills that responders need to function effectively in mass consequence events. NTED/TPP primarily serves state, local, territorial, and tribal entities in 18 professional disciplines. Instruction is offered at the awareness, performance, and management and planning levels. Students attend NTED/TPP courses to learn how to apply the basic skills of their profession in the context of preparing, preventing, deterring, responding to, and recovering from acts of terrorism and catastrophic events. Course subjects range from weapons of mass destruction terrorism, cybersecurity, and agro-terrorism to citizen preparedness and public works. NTED/TPP training includes multiple delivery methods: instructor-led (direct deliveries); train-the-trainers (indirect deliveries); customized (conferences and seminars); and web-based. Instructor-led courses are offered in residence (i.e., at a training facility) or through mobile programs, in which courses are brought to state and local jurisdictions that request the training. NTED/TPP through the Center for Homeland Defense and Security (CHDS) provides graduate and executive level educational programs and services focused 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.

- **National Exercise Program (NEP)** serves as the principal mechanism for examining the preparedness and readiness of the United States across the entire homeland security and management enterprise. The purpose of the NEP is to design, coordinate, conduct, and evaluate exercises that rigorously test the Nation's ability to perform missions and functions that prevent, protect against, respond to, recover from, and mitigate all hazards. As a component of the National Preparedness System, the NEP provides a consistent method to examine and validate federal and whole community partner core capabilities, which in turn indicate the Nation's progress in reaching the National Preparedness Goal (Goal).

  Each Program cycle consists of a two-year, progressive schedule of exercises that are selected based on their support to the Goal, and the Program's Principals' Objectives. The types of exercises selected into the program may include facilitated policy discussions, seminars and workshops, tabletop exercises, modeling and simulation, drills, functional exercises, and full-scale exercises. All of which may be sponsored by organizations from any level of government, the non-governmental and private sector, and the whole community.

Integrated Emergency Management Course (IEMC): Preparing Communities for a Complex Coordinated Attack is a four-day course designed to improve the ability of local jurisdictions to prepare for, protect against, and respond to complex coordinated attacks. The course focuses on engaging participants from multiple disciplines in a discussion and analysis of local, state, regional, and Federal capabilities required to respond to a coordinated attack against multiple targets. Through briefings, case studies, facilitated discussions, and planning workshops, participants work through a community-specific attack scenario to identify gaps in their current plans, as well as mitigation strategies. Similar to Joint Counterterrorism Awareness Workshop Series (JCTAWS), the course utilizes breakout groups and facilitation to assist the community in identifying these gaps. IEMC was developed for second tier metropolitan areas that may have fewer resources and less experience with counterterrorism operations. Seven more courses are scheduled in 2018. After the course, the self-identified gaps along with potential mitigation strategies and a list of available resources are presented to the community in a Summary Report.

The **Integrated Public Alert and Warning System (IPAWS)** is a national FEMA-managed system that public safety officials can use to send public information and warning messages to people in a specific geographic area. IPAWS connects authorities at the federal, state, local, tribal, and territorial levels and enables sending of Wireless Emergency Alert (WEA) messages to cell phones, Emergency Alert System (EAS) broadcasts to radio and TV, non-weather emergency message broadcasts over NOAA All-Hazards Weather Radio, and Internet applications and websites that support alert and warning distribution. IPAWS provides emergency information to people without an understanding of the English language and facilitates delivery of emergency information to people with access and functional needs. IPAWS is also connected with the Canadian Multi-Agency Situational Awareness System to enable sharing of alert, warning, and incident information across borders to improve response coordination during binational disasters. Additional information and

inquiries about IPAWS and requirements for becoming an IPAWS user can be directed to the IPAWS Program Office. For more information, visit https://www.fema.gov/integrated-public-alert-warning-system or contact IPAWS@fema.dhs.gov

Joint Counterterrorism Awareness Workshop Series (JCTAWS). The Joint Counterterrorism Awareness Workshop Series (JCTAWS) is a nationwide initiative designed to improve the ability of local jurisdictions to detect, prevent, and disrupt terrorist activities. JCTAWS have been held in more than 35 major cities across the U.S., bringing together Federal, state, and local participants from across the law enforcement, fire, emergency response, medical services, and private sector communities to include hospital and medical personnel. The workshops, emphasizing the state and local response, delve into the challenges presented by both the operational and medical responses, and aim to review existing preparedness, response and interdiction plans, policies, and procedures related to a complex terrorist attack; identify gaps in plans, operational capabilities, response resources, and authorities; examine healthcare system challenges unique to a complex attack; strategize about community and bystander assistance to the wounded and consider providing medical management nearer to the attack site; and identify federal, state, and local resources—including grants, training, exercises, and technical assistance—available to address potential gaps in capabilities.

Office of the Law Enforcement Advisor. The mission and role of FEMA's Senior Law Enforcement Advisor is to enhance communication and coordination between FEMA and the law enforcement community and provide the Administrator and Agency with a law enforcement perspective on plans and policies to support the agency's integration of law enforcement, public security, and emergency management communities.

Preparedness (Non-Disaster) Grant funding in the form of formula, competitive, and risk-based grants to enhance the capacity of state, local, tribal, territorial, and private sector emergency responders to prevent, protect against, respond to, and recover from terrorism and natural disasters, including a weapon of mass destruction, terrorism incident involving chemical, biological, radiological, nuclear, explosive devices, and cyber-attacks, as well as other disasters. For more information on how to find and apply for grants visit http://www.fema.gov/preparedness-non-disaster-grants or https://www.grants.gov/.

Protection and National Preparedness contributes to the development and implementation of preparedness doctrine that reaches federal state, local, tribal, and territorial emergency management communities, as well as non-government entities and the private sector. The guidance and doctrine includes the National Preparedness Goal and National Preparedness System, National Incident Management System, and National Planning Frameworks.

- Within its National Preparedness Directorate, the National Integration Center examines emerging technologies, develops state and local planning guidance, provides technical assistance, and supports resource typing and the credentialing of emergency response personnel.
- Within its National Continuity Programs, FEMA provides guidance and tools for continuity at all levels of government and provides an array of continuity communications capabilities to key partners. Continuity of Operations ensures an individual organization can continue to perform its essential functions, provide essential services, and deliver core capabilities during a disruption to normal operations.

Federal Law Enforcement Training Centers (FLETC)

***Contact Information*:**
Federal Law Enforcement Training Centers
Address: 1131 Chapel Crossing Road, Bldg. 2200, Glynco, GA 31524

Web Site:
https://www.fletc.gov/state-local-tribal

E-mail:
stateandlocaltraining@dhs.gov

The FLETC offers advanced and specialized law enforcement training in a variety of topics through the State, Local, and Tribal Division (SLTD), to state, local, tribal, and campus law enforcement officers throughout the U.S. and Indian country/jurisdictions. The programs SLTD delivers are developed with the advice, assistance, and support of federal, state, local, tribal, and campus law enforcement agencies and are updated to ensure relevance to today's issues. They are conducted at selected venues throughout the country hosted by a local law enforcement agency or at one of FLETC's training delivery points, which are located in Artesia, NM; Charleston, SC; Cheltenham, MD; and Glynco, GA. Tuition, lodging, and meals assistance may be available to state, local, and tribal officers, but attendance is on a "space-available" basis. To learn more about FLETC training courses available to state, local, tribal, and campus law enforcement and for contact information visit https://www.fletc.gov/state-local-tribal or contact stateandlocaltraining@dhs.gov.

eFLETC
In addition to in-residence training courses, FLETC expects to introduce in FY19 eFLETC. eFLETC is a new, cloud-based law enforcement online training environment that offers traditional, formal online training, as well as interactive, instructor-led courses that incorporate social learning, networking, and collaboration to fully enhance the learning experience. eFLETC will be available online, at the convenience of today's busy law enforcement officers and agents who have Regional Information Sharing System (RISS) Automated Trusted Information Exchange Application™ (ATIX).

The eFLETC course catalog will include an array of robust and awareness level training courses that are relevant for today's sworn and vetted law enforcement officers and agents. For information about eFLETC, including news and updates on the go-live date, please visit www.fletc.gov.

U.S. Immigration and Customs Enforcement (ICE)

ICE's primary mission is to promote homeland security and public safety through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration. The agency has an annual budget of approximately $6 billion dollars, primarily devoted to its two operational directorates – ICE Homeland Security Investigations (HSI) and ICE Enforcement and Removal Operations (ERO).

Continued Presence.
ICE may sponsor an application for Continued Presence (CP) submitted by a state or local law enforcement agency in cases where the victimization meets the federal definition of trafficking, as found in the Trafficking Victims Protection Act of 2000, Pub. L. No. 106-386, § 103(8) and 22 U.S.C. § 7102(8). When state or local law enforcement officials identify a victim of human trafficking, they should coordinate with their federal law enforcement partners to sponsor an application for CP. For more information, visit https://www.ice.gov/doclib/human-trafficking/pdf/continued-presence.pdf.

CP allows eligible aliens to temporarily remain in the United States for up to two years, with the possibility of extension, to facilitate an

investigation or prosecution of the human trafficking-related crimes committed against them. ICE has the final authority to grant, terminate, or deny CP to victims of severe forms of human trafficking who may be potential witnesses in the investigation or prosecution of those responsible for such trafficking. CP is a discretionary law enforcement tool utilized on a case-by-case basis as warranted and appropriate. For a trafficking victim who filed a civil action under 18 U.S.C. §1595 and meets these requirements, DHS shall grant or extend CP, subject to certain exceptions. CP may be requested by any law enforcement agency; however, submissions by state and local law enforcement agencies must be sponsored by a federal law enforcement agency.

Toolkit for Prosecutors. To demonstrate its commitment to strengthening coordination with state and local prosecutor partners, ICE developed the Toolkit for Prosecutors. This Toolkit is aimed at helping prosecutors navigate situations where important witnesses, victims, or defendants may face removal because they are illegally present in the United States. For more information, visit https://www.ice.gov/doclib/about/offices/osltc/pdf/tool-kit-for-prosecutors.pdf.

Victim Assistance Program (VAP) provides information and assistance to victims of federal crimes, including human trafficking, child exploitation, human rights abuses, and white collar crime. VAP also provides information to victims on post-correctional releases or removal of criminal aliens from ICE custody. VAP has developed informational brochures on human trafficking victim assistance, crime victims' rights, white collar crime, and the victim notification program. For further information, please contact VAP at victimassistance.ice@dhs.gov or 866-872-4973.

ICE's Victims Of Immigration Crime Engagement Office (VOICE) was created in 2017 as mandated by the Executive Order titled, *"Enhancing Public Safety in the Interior of the United States."*

The VOICE Office, which officially launched April 26, 2017, has several key objectives that include:

- Using a victim-centered approach to acknowledge and support victims and their families;
- Promoting awareness of available services to crime victims; and
- Building collaborative partnerships with community stakeholders assisting victims.

ICE established a toll-free hotline staffed with operators who triage calls to ensure victims receive the support they need. The number is 1-855-48-VOICE or 1-855-488-6423.

The type of assistance the VOICE Office offers includes:

- Establishing local contacts to help with unique victim requests;
- Linking victims with ICE Community Relations Officers who serve as local representatives to help victims understand the immigration enforcement and removal process;
- Providing access to social service professionals who are able to refer victims to local resources and direct service providers;
- Assisting individuals in signing up to receive automated custody status information through the DHS-Victim Information and Notification Exchange; and
- To the extent permitted by law or policy, providing information about the offender, including the offender's immigration status and custody status, and answering questions and concerns regarding immigration enforcement.

ICE ENFORCEMENT AND REMOVAL OPERATIONS (ERO)

The **287(g) Program** allows a state or local law enforcement entity to enter into a partnership with ICE, under a joint Memorandum of Agreement

(MOA), in order to receive delegated authority for immigration enforcement within their jurisdictions. In many cases, criminal activity is most effectively combatted through a multi-agency/multi-authority approach that brings together the skills and expertise of federal, state, and local resources. State and local law enforcement agencies play a critical role in protecting national security because the vast majority of criminals are taken into custody under their jurisdiction. The 287(g) Fact Sheet provides information regarding the 287(g) program. For more information, visit https://www.ice.gov/factsheets/287g-reform.

The **Criminal Alien Program (CAP)** provides ICE-wide direction and support in the biometric and biographic identification, arrest, and removal of priority aliens who are incarcerated within federal, state, and local prisons and jails, as well as at-large criminal aliens that have circumvented identification. The identification and processing of incarcerated criminal aliens, before release from jails and prisons, decreases or eliminates the time spent in ICE custody and reduces the overall cost to the Federal Government. Additionally, ICE ERO, in conjunction with the Offices of the United States Attorneys, actively pursues criminal prosecutions upon the discovery of offenses of the Nation's criminal code and immigration laws. This further enhances public safety and provides a significant deterrent to recidivism. For more information, visit https://www.ice.gov/criminal-alien-program.

ICE Enforcement and Removal Operations 101 (ERO 101) is a PowerPoint presentation compiled to introduce ICE ERO and its program offices. Though the slides themselves are not accessible to the public, the presentation can be delivered by any field office upon request. ICE ERO 101 is a condensed overview of ICE ERO programs and initiatives and is updated quarterly. In addition, each field office has area of responsibility-specific slides to accompany the overall ICE ERO 101 in order to provide a more focused look at ICE ERO in the local area. To find the nearest field office, visit https://www.ice.gov/contact/ero.

ICE ERO Most Wanted Program is managed by the National Fugitive Operations Program (NFOP) as a vital tool to support ICE ERO's efforts in the location and arrest of the most dangerous fugitives and at-large criminal aliens. The Most Wanted Program serves as a force multiplier by focusing additional resources on the most egregious offenders, develops community support by providing visibility and fostering awareness of ICE ERO's public safety mission, and builds cooperative relationships with law enforcement partners though the exchange of mutually beneficial information aimed at removing these threats from local communities. For more information, visit https://www.ice.gov/fugitive-operations and https://www.ice.gov/most-wanted.

ICE-INTERPOL Fugitive Alien Removal (FAR) Initiative. The FAR Initiative seeks to locate, arrest, and remove foreign fugitive aliens at-large in the United States. A "foreign fugitive" is a removable alien with an arrest warrant from a foreign country for an offense which is also considered a crime in the United States. ICE Liaisons at INTERPOL assist in confirming criminal warrants from foreign countries, developing investigative leads, and sharing information with law enforcement partners across borders. The ICE Liaisons at the INTERPOL Alien/Fugitive Division can be contacted at 202-532-4297 or 202-616-2416. The INTERPOL Operations and Command Center can be reached at 202-616-3900 or INTERPOL.ALIENFUGITIVEDIVISION@ice.dhs.gov.

Joint Effort Initiative. The Joint Effort Initiative combines the resources and expertise of ICE ERO with local law enforcement agencies to help make communities safer. The purpose of this initiative is to promote community safety through the arrest and removal

of criminal aliens and members of transnational street gangs. Working in a support role to local law enforcement, ICE ERO responds to situations where there is believed to be a criminal and immigration nexus, and provides investigative and enforcement support with the goal of reducing crime. Individual ICE ERO officers or a Fugitive Operations Team can embed in a state or local law enforcement agency on a part-time basis or in a full-time capacity. For more information, visit https://www.ice.gov/fugitive-operations.

Law Enforcement Information Sharing Initiative (LEISI) facilitates the systematic sharing of DHS unclassified biographic and biometric law enforcement information with other federal, tribal, state, local, and international law enforcement and immigration agencies. LEISI provides the electronic Law Enforcement Information Sharing Service (LEIS Service) that other law enforcement agencies can utilize to query records pertaining to ICE criminal subjects and ICE and CBP immigration violators. For more information, contact DHS-LEISI@ice.dhs.gov.

Law Enforcement Support Center (LESC), administered by ICE ERO, is a critical point of contact for the national law enforcement community, providing a wide range of information services to officers and investigators at federal, state, and local levels. The LESC operates 24 hours a day; 365 days a year to provide timely, accurate and real-time assistance to law enforcement agencies that are in need of the immigration status and identities of a foreign national who has been encountered, arrested, or is under investigation for criminal activity.

To support these law enforcement efforts, the most efficient method to request and receive immigration information is by submitting an Immigration Alien Query (IAQ) to the LESC. The IAQ is generated in two ways: either by an automated biometric (fingerprints) submission; or by a biographic submission, initiated by utilizing the International Justice and Public Safety Network (Nlets), message key IAQ at VTICE0900. Direct contact can also be made via the Law Enforcement Hotline at 1-802-872-6020. For additional information, visit https://www.ice.gov/lesc.

National Criminal Analysis and Targeting Center (NCATC). As part of ICE ERO's Targeting Operations Division, the NCATC analyzes data and develops lead and information referrals for law enforcement. The information is used to protect the safety and security of the public by assisting in the process of locating and arresting aliens who pose a threat to the nation's communities. By leveraging technology and partnerships with domestic and international law enforcement, regulatory, and intelligence agencies, the NCATC devotes a specialized law enforcement workforce that analyzes the nature and characteristics of the removable alien population. The NCATC, in coordination with ERO and other law enforcement entities, serves as a critical operational component in fulfilling ICE's mission.

National Fugitive Operations Program (NFOP) was established to locate and arrest removable aliens who are at-large within the United States. The 129 Fugitive Operations Teams (FOTs) across the Nation prioritize their investigations on national security cases and transnational gang members, convicted criminals and sex offenders, visa violators, and aliens with removal orders who have failed to depart the United States. FOT members work together with law enforcement partners and on interagency task forces to offer immigration enforcement expertise and pursue a common public safety strategy. For more information, visit https://www.ice.gov/fugitive-operations.

Online Detainee Locator System (ODLS) is a public system available online at https://www.ice.gov/lesc that allows family members, legal

representatives, and members of the public to locate immigration detainees who are in ICE detention. As part of detention reform, ICE deployed the ODLS so that family members and attorneys can locate detainees more easily online, 24 hours a day, seven days a week. The system is available in eight different languages, with more languages to follow. The ODLS can be searched in two ways: 1) by Alien Registration number (or A-number, the nine-digit identification number assigned to a person who applies for immigration benefits or is subject to immigration enforcement proceedings); or 2) by last name, first name, and country of birth. For more information, visit https://locator.ice.gov/odls/homePage.do.

Probation and Parole Enforcement entails the identification and arrest of foreign born nationals who have been convicted of crimes and released from incarceration (paroled), or have been placed on probation without incarceration and released into the community under supervision. This is an essential immigration enforcement function of ICE in carrying out its public safety mission. ERO Officers and Fugitive Operations Teams work closely with probation and parole agencies to serve as a force multiplier, provide an open exchange of information, and fulfill common community safety objectives.

The Pacific Enforcement Response Center (PERC) provides 24/7 mission critical support to ICE field offices by delivering near real-time detainer issuance, intelligence support, and proactive and risk-based targeting of removable criminal aliens. This is accomplished through interoperability and the information sharing capabilities of the PERC, the LESC, and the FBI's Next Generation Initiative (NGI) fingerprint database. The PERC's proactive targeting focuses on removable criminal aliens who pose a threat to national security and public safety. Real-time intelligence is disseminated to field offices in the form of actionable leads associated with criminal aliens in federal/state/local custody and at-large aliens. In addition, the PERC provides critical information to INTERPOL, Joint Terrorism Task Forces, and other federal law enforcement partners in furtherance of shared public safety and national security missions. The PERC can be contacted directly 24/7 by calling the Law Enforcement Line at 949-360-4500.

ICE HOMELAND SECURITY INVESTIGATIONS (HSI)

Border Enforcement Security Task Force (BEST) The primary mission of the ICE HSI BEST is to combat emerging and existing Transnational Criminal Organizations (TCO) by employing the full range of federal, state, local, tribal, and international law enforcement resources in the fight to identify, investigate, disrupt and dismantle these organizations at every level of operation along U.S. international borders (land, air, and seaports). To date, there are currently 57 BESTs positioned along U.S. international borders located across 21 states and Puerto Rico, in which special agents, task force officers, and task force personnel investigate a wide range of criminal activity with a nexus to the border, to include drug trafficking, arms trafficking, human trafficking and smuggling, gangs, child exploitation, money laundering and bulk cash smuggling, maritime smuggling, illicit tunnels, and commercial fraud. These BESTs are comprised of approximately 1,200 members representing more than 150 federal, state, local, tribal, and international law enforcement agencies that have jointly committed to investigate transnational criminal activity. For more information, visit https://www.ice.gov/best.

Counter-Proliferation Investigations Program (CPI) oversees a broad range of investigations related to export law violations. CPI targets the trafficking and illegal export of conventional military equipment, firearms, controlled dual use equipment and technology, and materials used to manufacture weapons of

mass destruction, including chemical, biological, radiological, and nuclear materials. ICE HSI Special Agents enforce all U.S. export laws involving military items and controlled dual-use goods, as well as products going to sanctioned or embargoed countries. For more information, visit https://www.ice.gov/cpi.

The Counterterrorism and Criminal Exploitation Unit (CTCEU) focuses on preventing criminals and terrorists from exploiting the nation's immigration system. CTCEU primarily investigates nonimmigrant visa holders who overstay their authorized period of admission or violate the terms of their admission, and pose a potential national security or public safety concern. CTCEU places the highest priority on scrutinizing the activities of known or suspected terrorists and terrorist associates, and on combating the criminal exploitation of the student visa system. For more information, please contact the CTCEU at ctceu@ice.dhs.gov.

Cultural Property, Art and Antiquities Program (CPAA) oversees investigations involving the illicit trafficking of cultural property from countries around the world and facilitates the repatriation of these objects to their rightful owners. United States federal importation laws regarding smuggling and trafficking provide ICE HSI special agents the authority, jurisdiction, and responsibility to take the leading role in criminal investigations that involve the illicit importation and distribution of stolen or looted cultural property and prosecuting those responsible for these crimes. When contacting ICE HSI to report instances of illicit importation and distribution of cultural property, please provide as much detailed information and supporting documentation as possible, including the following: a detailed description of the artifact and location (pictures if possible); a full statement of the reasons for the belief that the artifact may be or has been imported into the United States due to the illicit importation from (1) country of origin (if known) or (2) distribution from an archeological site in the United States (if known). For more information, visit https://www.ice.gov/cultural-art-investigations. Reports may be sent to HSIculturalproperty@ice.dhs.gov.

Cyber Crimes Center (C3), was established in 1997 for the purpose of combating crimes committed on, or facilitated by, the Internet. C3 is ICE HSI's main contact point for coordinating the agency's cyber strategy as it relates to cybercrime and computer forensics. ICE HSI's primary strategy for cybercrime is to combat transnational cybercrime threats and the criminal exploitation of the Internet by investigating, disrupting, and dismantling transnational criminal organizations and other malicious actors engaged in high-impact or far-reaching cybercrime, as well as providing training, guidance, and assistance to ICE HSI offices located throughout the world.

C3 is comprised of the Cyber Crimes Unit (CCU), the Child Exploitation Investigation Unit (CEIU), and the Computer Forensics Unit (CFU). This state-of-the-art center offers cyber-crime support and training to federal, state, local, and international law enforcement agencies. C3 also includes a fully equipped computer forensics laboratory, which specializes in digital evidence recovery. For more information, visit https://www.ice.gov/cyber-crimes.

Document and Benefit Fraud Task Forces (DBFTF). ICE HSI leads 29 interagency DBFTFs across the United States. Individual task forces are comprised of federal, state, and/or local law enforcement partners working together to combat immigration document and benefit fraud, as well as related criminal violations. DBFTF locations include Atlanta, Baltimore, Boston, Buffalo, Chicago, Dallas, Denver, Detroit, El Paso, Harlingen, Houston, Honolulu,

Los Angeles, Miami, New York, Newark, New Orleans, Orlando, Philadelphia, Phoenix, Sacramento, Salt Lake City, San Antonio, San Diego, San Francisco, San Juan, Saint Paul, Seattle, and Washington, D.C. Through collaboration and partnership with multiple federal, state, and local agencies, the DBFTFs maximize resources, eliminate duplication of efforts, and produce a strong law enforcement presence. They combine ICE HSI's unique criminal and administrative authorities with a variety of other law enforcement agencies' tools and authorities to achieve focused, high-impact criminal prosecutions and financial seizures. Partners include U.S. Citizenship and Immigration Services, Fraud Detection and National Security; U.S. Department of State, Diplomatic Security; U.S. Department of Labor, Office of the Inspector General; U.S. Social Security Administration, Office of the Inspector General; U.S. Postal Inspection Service; U.S. Secret Service; and numerous state and local law enforcement agencies. Supporting these task forces are the ICE HSI Forensic Laboratory and the ICE HSI Cyber Crimes Center (C3). For more information, visit https://www.ice.gov/identity-benefit-fraud.

Forced Labor Program. ICE HSI investigates allegations of forced labor in violation of the Tariff Act of 1930 (Title 19 U.S.C. §1307), relating to the illegal importation of goods mined, manufactured, or produced, wholly or in part, through the use of forced labor, prison labor, and/or indentured labor under penal sanctions. When contacting ICE to report instances of forced labor, please provide as much detailed information and supporting documentation as possible, including the following: a full statement of the reasons for the belief that the product was produced by forced labor and that it may be or has been imported into the United States; a detailed description of the product; and all pertinent facts known regarding the production of the product abroad. Reports may be emailed to ICE.ForcedLabor@ice.dhs.gov.

Human Rights Violators and War Crimes Center (HRVWCC) is a multi-agency program directed by ICE HSI with partners from the FBI, Department of State, USCIS and ICE's Human Rights Law Section. HRVWCC conducts investigations focused on human rights violations in an effort to prevent the United States from becoming a safe haven to those individuals who engage in the commission of war crimes, genocide, torture, and other forms of serious human rights abuses from conflicts around the globe. Individuals seeking to report these abuses of human rights may contact the center at hrv.ice@dhs.gov. For additional information, visit https://www.ice.gov/human-rights-violators-war-crimes-unit.

The DHS **Human Smuggling Cell (HSC)** was established on October 1, 2014, in accordance with the White House National Security Council's mandate that law enforcement and the intelligence community collaborate and share intelligence and other information regarding human smuggling. The HSC is comprised of analytic and operational groups that collaborate to operationalize intelligence leading to the identification and disruption of human smuggling organizations, and also to provide strategic oversight on illegal migration trends. The HSC provides leadership and guidance to a number of initiatives in an effort to thwart the illegal movement of Special Interest Aliens. Among these is the Extraterritorial Criminal Travel (ECT) Program. The ECT Program was created in June 2006 as a joint partnership between ICE HSI and the U.S. Department of Justice, Criminal Division, Human Rights and Special Prosecutions Section to address U.S. security risks posed by transnational human smuggling organizations.

ICE HSI Department of Motor Vehicles (DMV) Outreach was developed to raise awareness about corruption at DMV facilities. A principal component of the campaign is to alert DMV

employees, law enforcement, and the public to the seriousness of fraud schemes perpetrated at DMV facilities. By adding education and outreach components, ICE HSI and its partners work together to deter the crime from happening, encourage people to report the crime, and ensure that their investigations are comprehensive and more efficient. Outreach materials, including posters, brochures, and short videos were developed by ICE HSI to support the outreach and are utilized by nearly every U.S. jurisdictional (state) and territorial DMV in employee new-hire and refresher ethics training. The materials provide guidance to DMV employees by promoting accountability and vigilance in an effort to reduce corruption and preserve the integrity of the DMV process. For more information, email ibfu-ice-hq@dhs.gov.

ICE HSI Forensic Laboratory (ICE HSI-FL) provides forensic, intelligence, and investigative support to ICE HSI, DHS, and many other U.S. and foreign law enforcement agencies. The ICE HSI-FL is accredited by the American National Standards Institute – American Society of Quality (ANSI-ASQ) National Accreditation Board (ANAB) under the International Standards ISO/IEC 17025. Forensic disciplines include questioned document and latent print examination. Additionally, the ICE HSI-FL provides intelligence alerts, reference material on travel and identity documents, and fraudulent document detection training. The ICE HSI-FL manages the ICE HSI Polygraph Program and oversees the ICE HSI Evidence Recovery Team Program. For more information, visit https://www.ice.gov/hsi-fl.

ICE HSI International Operations Overseas Offices represent DHS's largest investigative law enforcement presence overseas. ICE HSI deploys more than 240 special agents and 156 Foreign Service nationals to 65 attaché offices in 46 countries in addition to liaison officers assigned to the 8 Department of Defense Combatant Commands. These agents enforce U.S. customs and immigration laws to protect the United States and its interests from terrorism and illicit trade, travel, and finance by conducting international law enforcement operations and removals.

The mission of ICE HSI International Operations is threefold: (1) Support domestic operations by conducting and coordinating investigations with foreign counterparts; (2) Disrupt transnational criminal organizations before they can bring illicit products, people, and proceeds into or out of the United States; (3) Build on international partnerships and increase foreign capacity through outreach and training.

To locate or contact an ICE HSI International Office, visit https://www.ice.gov/contact/hsi-international-ops.

You may also go through the ICE HSI domestic office in your jurisdiction or the 24/7 hotline at 866-347-2423 (from U.S. and Canada) or 802-872-6199 (from any country in the world).

ICE HSI Tip Line is an internationally accessible venue through which the public, as well as federal, state, and local law enforcement agencies, can report suspected violations of ICE HSI-investigated immigration and customs laws. Special agents and intelligence research specialists assigned to the Tip Line take reports 24 hours a day, 365 days a year, and have the capability to customize questions to meet the needs of national enforcement priorities. Phone toll free 866-347-2423 from the U.S. and Canada, or from any country in the world phone 802-372-6199. For more information, visit https://www.ice.gov/webform/hsi-tip-form.

The **International Organized Crime Intelligence and Operations Center (IOC-2)** supports member agency efforts to disrupt and dismantle transnational criminal organizations (TCO) posing the greatest threat to the United States. This mission is accomplished through the deconfliction of member agency

investigative endeavors; dissemination of leads and intelligence; coordination of multi-agency and multi-national law enforcement operations, investigations, prosecutions, and forfeiture proceedings; and the provision of operational funding. IOC-2 focuses primarily on TCOs involved in non-drug centric crime, such as money laundering, credit card fraud, weapons trafficking, identity theft, fraud scams, cybercrime, and human smuggling/trafficking. To facilitate its efforts, the IOC-2 leverages the resources of its ten member agencies, the OCDETF Fusion Center, the Special Operations Division, and other domestic and international resources. IOC-2 is limited to providing support to member agencies only; however, state and local law enforcement officers assigned to task forces operated by member agencies can utilize its capabilities.

National Bulk Cash Smuggling Center (BCSC) is a 24/7 operations and intelligence facility providing real-time tactical intelligence and investigative support to the federal, state, and local officers involved in enforcement and interdiction of bulk cash smuggling and the transportation of illicit proceeds. This is accomplished through the examination and exploitation of evidence obtained at the borders, during traffic interdictions, and other law enforcement encounters. The BCSC targets transnational criminal organizations that seek to avoid traditional financial institutions by repatriating illicit proceeds through an array of methods, including commercial and private aircraft, passenger and commercial vehicles, maritime vessels, and pedestrian crossings at U.S. land borders. For more information, visit https://www.ice.gov/bulk-cash-smuggling-center or contact BCSC@dhs.gov or 866-981-5332.

National Intellectual Property Rights Coordination Center (IPR Center) stands at the forefront of the U.S. government's response to global intellectual property theft and enforcement of its international trade laws. The IPR Center helps ensure national security by protecting the public's health and safety, the U.S. economy, and U.S. warfighters by stopping predatory and unfair trade practices that threaten the global economy. The IPR Center is led by an ICE HSI director, along with deputy directors from ICE HSI, the FBI, and CBP. The center brings together 23 partner agencies in a task force structure consisting of 19 key federal agencies, INTERPOL, EUROPOL, and the governments of Canada and Mexico.

The IPR Center leverages the resources, skills, and authorities of each partner, so as to provide a comprehensive response to intellectual property theft. For more information, visit https://www.iprcenter.gov/. For additional information on available training opportunities, contact IPRCenter@dhs.gov.

Operation Community Shield is the ICE HSI anti-gang initiative combining ICE's expansive statutory and administrative enforcement authorities to combat the growth and proliferation of transnational criminal street gangs, prison gangs, and outlaw motorcycle gangs throughout the United States in cooperation with federal, state, local, tribal, and foreign law enforcement partners. With these partners, ICE HSI enhances intelligence gathering and information sharing, exploits 21st century law enforcement technology, and capitalizes on a worldwide presence to combat these global criminal networks and mitigate the threats they pose to the public safety and national security of the United States and other countries. For more information, visit https://www.ice.gov/national-gang-unit.

The **Organized Crime Drug Enforcement Task Force Fusion Center (OFC)** fosters increased communication, cooperation, and coordination between member agencies through the provision of target deconfliction and direct intelligence support to ongoing HSI investigations. The OFC utilizes a consolidated database consisting of over 700 million law enforcement, regulatory, and immigration records to

generate intelligence products for field exploitation. OFC is limited to providing support to member agencies only; however, state and local law enforcement officers assigned to task forces operated by member agencies can utilize its capabilities.

Parole and Law Enforcement Programs Unit (PLEPU) holds the final authority to grant, terminate, or deny all Significant Public Benefit Paroles (SPBP) for law enforcement purposes. SPBP is a law enforcement tool that may be requested by any law enforcement agency or prosecutors on behalf of persons of law enforcement interest who are foreign nationals, are inadmissible to enter the United States, and are needed to assist and/or participate in administrative, judicial, or legislative proceedings, and/or investigations. SPBP is a mechanism that allows otherwise inadmissible aliens to enter the United States and remain therein for a limited time and purpose. For more information on the SPBP program, please contact the local ICE HSI field office.

Shadow Wolves. The ICE HSI Shadow Wolves are Native American Tactical Officers assigned to the Tohono O'odham Nation in Arizona to enforce immigration and customs laws and regulations. This reservation contains 2.8 million acres of land and includes a 75-mile-long stretch of the U.S. border with Mexico. The Shadow Wolves use their unique language and tracking skills to interdict and investigate contraband and have assisted law enforcement with the investigation of kidnappings, the deaths of illegal aliens, sexual assaults, missing children, and any reports of border violence. The Shadow Wolves have traveled to the Blackfeet Indian Reservation and the Bay Mills Chippewa Indian Reservation to share their expertise. Further, the Shadow Wolves have conducted training with the U.S. Department of Defense in several of the former Soviet Republics to teach the ancient art of tracking to combat nuclear proliferation from the former Soviet Republics. For additional information, please contact 800-973-2867 and ask to speak with the Unit Chief for the ICE HSI Contraband Smuggling Unit in Washington, D.C. For more information, visit https://www.ice.gov/factsheets/shadow-wolves.

Title 19 Cross-Designation. Title 19, section 1401 of the U.S. Code provides a mechanism for ICE HSI to designate federal, state, local, tribal, and foreign law enforcement officers as "Customs Officers". The unique resources and subject matter expertise of these officers complement ICE HSI investigations to effectively combat transnational crime. Law enforcement officers cross-designated under 19 U.S.C. §1401(i) harness their invaluable experience with this unique federal authority to collectively enhance joint investigations of contraband smuggling, money laundering, and fraud-related activities, which disrupt and dismantle criminal organizations threatening this country's borders. With this authority, Title 19 cross-designated officers have the ability to execute and serve arrest warrants, subpoenas, and summonses in compliance with customs laws, as well as carry firearms in compliance with ICE HSI firearms policy. For more information on the Title 19 Program Directive, please contact 800-973-2867 to speak with the Unit Chief for the ICE HSI Contraband Smuggling and Gang Unit in Washington, D.C., or email the unit at HSITFO@ice.dhs.gov. For additional information, visit https://www.ice.gov/customs-cross-designation.

Trade Transparency Unit (TTU) is a key component in ICE HSI's strategic efforts to combat and prevent Transnational Criminal Organizations (TCOs) from exploiting international trade and financial systems to disguise, move, and launder illicit funds and proceeds, a scheme commonly known as trade-based money laundering (TBML). The TTU uses ICE HSI's unique authorities to access financial and international trade data to

identify financial irregularities and international trade anomalies indicative of TBML, customs fraud, contraband smuggling, and other financial crimes. For more information, visit https://www.ice.gov/trade-transparency.

Office of Intelligence and Analysis (I&A)

I&A is a member of the national Intelligence Community (IC) and ensures that information related to homeland security threats is collected, analyzed, and disseminated to the full spectrum of homeland security partners in the Department; at federal, state, local, tribal, and territorial levels; in the private sector; and in the IC.

I&A works closely with Department Component intelligence organizations, as well as state, local, tribal, territorial, and private sector entities to ensure non-traditional streams of information are fused with traditional IC sources to provide a complete assessment of threats to the homeland.

The Under Secretary for Intelligence and Analysis, in the capacity of Chief Intelligence Officer for DHS, implements a mandate to integrate the Department's intelligence components and functions—the DHS Intelligence Enterprise—by driving a common intelligence mission.

I&A is the Executive Agent for coordinating federal support for state and major urban area fusion centers. It also leads the Department's information sharing efforts. I&A works to solidify productive and collaborative relationships with its partners to enhance information sharing. This collaboration and coordination is bolstered by the assignment of I&A field personnel at state and major urban area fusion centers, as well as other strategic locations, providing direct intelligence support to key state, local, tribal, and territorial partners, and private sector partners. These services include engagement and intelligence and information sharing support, intelligence analysis, and intelligence collection and reporting.

Counterintelligence Fundamentals Workshop (CIFWS) is a training initiative offered by the DHS Counterintelligence Division (CIPD) to provide a one-day, on-site workshop to fusion centers as a means of promoting counterintelligence awareness to fusion centers personnel. The CIFWS program is intended to familiarize students with the potential intelligence collection threat directed against their facility, and state, local, tribal, and territorial officials. This training also equips attendees with the ability to recognize an elicitation attempt or recruitment pitch. Prior to the training, CIPD notifies the I&A field representative assigned to the fusion center of training intent, potential training dates, and logistic requirements for this effort. I&A field representatives are responsible for coordinating with their local FBI counterparts and promoting the event to their state, local, tribal, and territorial counterparts; as well as to other DHS representatives.

DHS Open Source Enterprise Daily Intelligence Reports
These daily and weekly reports provide priority intelligence requirements on multiple topics of interest to facilitate a greater understanding of the nature and scope of threats and hazards to the homeland. They are provided to federal, state, local, tribal, territorial, and private sector officials to aid in the identification and development of appropriate actions, priorities, and follow-on measures. These reports may be accessed via the HSIN. To access or sign-up for HSIN, visit http://www.dhs.gov/homeland-security-information-network-hsin.

Fusion Process Technical Assistance Program. Effective prevention efforts depend on the ability of all levels and sectors of government, as well as private industry, to collect, analyze, disseminate, and use homeland security and crime-related information and intelligence. Accordingly, the establishment of a network of fusion centers to facilitate

effective nationwide information sharing has been a top priority. The Fusion Center Technical Assistance Program hosts in-person small group meetings of peer SMEs to conduct collaborative discussions on best practices, lessons learned, and expectations associated with the effective development and implementation of specific operational capabilities. To learn more or to apply for assistance, visit FusionCenterTA@anl.gov.

HSDN Resources for State and Local Partners. Appropriately-cleared state and local personnel assigned to fusion centers are granted access to Secret-level network resources via the Homeland Secure Data Network (HSDN). These resources include intelligence products from I&A that are hosted on HSDN, as well as a range of other resources such as access to the National Counterterrorism Center Current portal for counter-terrorism information, the DEA portal for counternarcotics intelligence, and a number of Department of Defense sites including cybersecurity, counterterrorism, intelligence, and counternarcotics information.

The **DHS Intelligence Training Academy (ITA)** develops and delivers homeland security intelligence training programs supporting the DHS intelligence enterprise, as well as the greater homeland security enterprise. The ITA is located in Washington, D.C. and also deploys mobile training teams in support of state, local, tribal, and territorial partners. The ITA is fully accredited by the Federal Law Enforcement Training Accreditation Board. To learn more, obtain a copy of the ITA Catalog, or to request training, contact IA-Registrar@hq.dhs.gov.

The **Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)** was established to enhance the abilities of fusion centers and law enforcement to easily share specific potential indicators of terrorist activity in order to prevent terrorist threats. The NSI training strategy is designed to increase the effectiveness of state, local, tribal, and territorial law enforcement and homeland security professionals in identifying, reporting, evaluating, and sharing pre-incident terrorism indicators to identify and prevent acts of terrorism. The NSI offers a host of customized online training for law enforcement and several other specific partner sectors. The training is designed to illustrate the importance of reporting suspicious activity linked to pre-operational behaviors that are indicative of terrorist activity, the attendant privacy protections, practical case examples, and directions on how to report SAR. NSI resources and training may be accessed by visiting its website at https://www.ncirc.gov.

National Protection and Programs Directorate (NPPD)

NPPD leads the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure.

BIOMETRIC IDENTITY MANAGEMENT

Office of Biometric Identity Management (OBIM) Automated Biometric Identification System (IDENT). The IDENT system matches, stores, and shares fingerprints of more than 200 million unique identities for immigration, border management, law enforcement, credentialing, and national security purposes. IDENT is interoperable with the FBI's Next Generation Identification (NGI) system and provides state, local, tribal, and territorial law enforcement with access to IDENT information via NGI.

OBIM Biometric Support Center (BSC) provides expert fingerprint identification services in support of DHS's Automated Biometric Identification System, which contains the fingerprints of more than 200 million individuals. The BSC performs manual fingerprint comparisons to identify both known and unknown individuals (e.g.

deceased subjects, cold cases). The BSC operates 24 hours a day/7 days a week. For additional information, contact afis@dhs.gov.

CHEMICAL SECURITY

Chemical Facility Anti-Terrorism Standards (CFATS). The CFATS program is the Department's regulatory program focused specifically on security at high-risk chemical facilities not located on navigable waterways. The program identifies and regulates high-risk chemical facilities to ensure they have security measures in place to reduce the risks associated with these chemicals. DHS chemical security inspectors work in all 50 states to help ensure facilities have security measures in place to meet security risk-based performance standards. For more information, contact CFATS@hq.dhs.gov.

COUNTER-IMPROVISED EXPLOSIVE DEVICE (IED) PROGRAMS AND RESOURCES

Counter-IED and Risk Mitigation Training. To reduce risk to the Nation's critical infrastructure, DHS's Office for Bombing Prevention (OBP) develops and delivers a diverse portfolio of counter-IED awareness solutions and training courses to build nationwide counter-IED capabilities and enhance awareness of IED threats. Coordinated through DHS Protective Security Advisors, State Homeland Security Officials and training offices, OBP courses educate federal, state, local, tribal, and territorial participants, such as municipal officials and emergency managers, state and local law enforcement and other emergency services, critical infrastructure owners and operators, and security staff on strategies to prevent, protect against, respond to, and mitigate bombing incidents. All training courses offered by OBP are available at no cost, comply with American National Standards Institute (ANSI) and International Association for Continuing Education and Training (IACET) standards, and are certified for Continuing Education Units (CEUs) through the Center for Domestic Preparedness. Available courses are listed below. For more information, visit https://www.dhs.gov/bombing-prevention-training. To request training, contact your local Protective Security Advisor (PSA) or contact OBP@hq.dhs.gov.

Direct Delivery In-Person Training

- Bomb Threat Management Planning Course (MGT-451)
- Bombing Prevention Awareness Course (AWR-348)
- IED Search Procedures Course (PER-339)
- Protective Measures Course (PER-336)
- Surveillance Detection Course for Bombing Prevention (PER-346)
- Vehicle Borne IED (VBIED) Detection Course (PER-312)

Virtual Instructor Led Training (VILT)

- Homemade Explosives (HME) and Precursor Awareness Course (AWR-338)
- Introduction to the Terrorist Attack Cycle Course (AWR-334)
- IED Construction and Classification Course (AWR-333)
- IED Explosive Effects Mitigation Course (AWR-337)
- Protective Measures Awareness Course (AWR-340)
- Response to Suspicious Behaviors and Items Course (AWR-335)

Independent Studies

- IED Awareness and Safety Procedures (AWR-341)
- Homemade Explosives and Precursor Chemicals Awareness for Public Safety (AWR-349)

Bomb-Making Materials Awareness Program (BMAP) is a national outreach program, sponsored by DHS in partnership with the FBI, designed to increase public and private sector awareness of the potential illicit use of HME precursor chemicals, explosive powders, and IED components. Through increased awareness,

BMAP builds a network of vigilant and informed private sector partners who serve as the Nation's counter-IED "eyes-and-ears" as the first line of defense in providing early detection of the sale of HME precursor chemicals.

Counter-IED Awareness Products are made available from OBP and can be found at https://www.dhs.gov/bombing-prevention-training.

- Counter-IED Awareness Cards & Posters
- DHS-DOJ Bomb Threat Guidance Brochure
- DHS Bomb Threat Procedures Checklist
- DHS-DOJ Bomb Threat Stand-off Card
- *FiRST* Smartphone Application
- Sports and Entertainment Venues Bombing Prevention Solutions Portfolio
- Protective Measures Guidance
- VBIED Identification Guide: Parked Vehicles
- Vehicle Inspection Guide (VIG) & Video

The **Multi-Jurisdiction Improvised Explosive Device Security Planning (MJIEDSP)** program is a systematic process that fuses counter-IED capability analysis, training, and planning to enhance urban area IED prevention, protection, mitigation, and response capabilities. The MJIEDSP assists with collectively identifying roles, responsibilities, capability gaps, and how to optimize limited resources within a multi-jurisdictional planning area. OBP works closely with communities to provide expertise on planning and operational requirements for IED incident preparedness in alignment with the National Preparedness Goal and Core Capabilities. For more information, contact OBP@hq.dhs.gov.

The **National Counter-IED Capabilities Analysis Database (NCCAD)** is an assessment program that uses a consistent and repeatable analytical methodology to assess and analyze the capabilities of bomb squads, explosives detection canine, dive, and SWAT teams throughout the United States. NCCAD assessments measure the capability elements of personnel, equipment, and training required for effective prevention, protection, and response to IED threats. This integrated information provides a snapshot of unit, state, regional, and national counter-IED preparedness that informs decision makers on policy decisions, resource allocation for capability enhancement, and crisis management. For more information, contact OBP@hq.dhs.gov.

Technical Resource for Incident Prevention (TRIP*wire*) is the DHS secure, online, collaborative information and resource-sharing portal for the Nation's security and emergency services professionals across the federal, state, local, and tribal sectors to increase awareness of evolving terrorist IED tactics, techniques, and procedures, as well as incident lessons learned and counter-IED preparedness information. Developed and maintained by OBP, the system combines expert analyses and reports with relevant documents, images, and videos gathered directly from terrorist sources to help users anticipate, identify, and prevent IED incidents. TRIP*wire* is available at no cost to registered subscribers and features a publicly accessible homepage with valuable preparedness information for the entire bombing prevention community at https://tripwire.dhs.gov. For additional information, contact OBP@hq.dhs.gov.

CYBERSECURITY

Automated Indicator Sharing (AIS) program is a machine-to-machine capability that receives, processes, and disseminates cyber threat indicators and defensive measures in real time to federal and non-federal partners.

AIS enables the National Cybersecurity & Communications Integration Center to receive indicators and remove personally identifiable information and other sensitive information not directly related to the cybersecurity threat, and to share cyber threat indicators

and defensive measures to partners. All federal and non-federal entities, as well as foreign government and foreign private-sector entities, may participate in the AIS initiative. For more information, visit https://www.dhs.gov/ais.

The **Continuous Diagnostics and Mitigation (CDM) Program** enables federal, state, local, and tribal governments to obtain the risk-based, cost-effective tools and capabilities they need to fortify their IT systems and government networks. CDM allows system administrators to know the state of their respective network at any given time, and identify flaws for priority resolution at near-network speed, resulting in lower operational risk/exploitation.

DHS, in partnership with the General Services Administration (GSA), established a government-wide acquisition vehicle for CDM—the CDM Tools and Continuous Monitoring as a Service (CMaaS) blanket purchase agreement (BPA)—which is available to federal, state, local, and tribal government entities. BPA participants achieve cost savings through tiered-price and task order discounts, enabling more efficient use of financial resources.

State and local governments may use the Direct Order/Direct Bill option to procure products/services from the CDM BPA via the delegated procurement authority, GSA Federal Systems Integration and Management Center (FEDSIM). For specific ordering options, visit GSA's 2013 CDM/CMaaS Ordering Guide at https://www.gsa.gov/portal/content/177883.

For more information about CDM, visit:

- www.gsa.gov/cdm for ordering information.
- www.us-cert.gov/cdm for operational information.
- www.dhs.gov/cdm for the CDM public website.

The CDM Program also offers a secure community of interest for stakeholders, hosted on the HSIN. To request membership, email the CDM Program at cdm.fnr@hq.dhs.gov.

Cyber Resiliency Review (CRR) is an assessment that the Cyber Security Evaluation Program offers to measure and enhance the implementation of key cybersecurity capacities and capabilities of critical infrastructure. The purpose of the CRR is to gather information regarding cybersecurity performance from specific critical infrastructure in order to gain an understanding of the relationships and impacts of infrastructure performance in protecting critical infrastructure operations. The results can be used to evaluate a provider independent of other assessments, used with regional studies to build a common perspective on resiliency, and used to examine systems-of-systems (i.e., large and diverse operating and organizing models). The key goal of the CRR is to ensure that core process-based capabilities exist, are measureable, and are meaningful as predictors for an organization's ability to manage cyber risk to national critical infrastructure. For more information about the CRR, contact the Cybersecurity Evaluation Program (CSEP) at CSE@dhs.gov.

Cyber Security Advisors (CSAs)

NPPD created the Cyber Security Advisor (CSA) Program in recognition of how a regional and national focused cybersecurity presence is essential to protect critical infrastructure. CSAs offer immediate and sustained assistance to prepare and protect state, local, territorial, and tribal governments and private sector entities. CSAs bolster the cybersecurity preparedness, risk mitigation, and incident response capabilities of these entities and bring them into closer alignment with the Federal government. CSAs represent a front-line approach and promote resilience of key cyber infrastructure throughout the U.S. and its territories. CSAs are regionally located DHS personnel assigned to districts throughout the U.S., with at least one per the 10 CSA regions, which are aligned to the Federal regions. Currently, the Cyber Security Advisors provide six types of services:

- Cyber Protective Visits: On-site meetings with an organization to answer questions, exchange information, and address concerns about cybersecurity;
- Educational and Awareness Briefings: Community-of-interest, symposium, and conference-focused briefings and workshops to help improve cybersecurity awareness and posture, while providing timely and relevant information on DHS and regional programs and activities;
- Assessments;
- Cyber Resilience Review (CRR);
- Cyber Infrastructure Survey Tool (C-IST): An expert-led, interview-based assessment focusing on over 80 cybersecurity controls; and
- Incident Response: Facilitate cyber incident response and provide Federal coordination for incident notification, containment, and recovery.

Please address CSA inquiries to: cyberadvisor@hq.dhs.gov.

Cybersecurity Information Products provide current cybersecurity information and recommended security practices to help users understand cybersecurity issues and mitigation options. This information enables users to reduce their exposure and susceptibility to cyber-attacks and exploits. For a complete list and access to cybersecurity information products, visit https://www.us-cert.gov/security-publications and https://ics-cert.us-cert.gov/Information-Products.

Cybersecurity Information Sharing and Collaboration Program (CISCP) is a voluntary information-sharing and collaboration program with and among critical infrastructure partners and the federal government to leverage trust for enhanced information sharing and collaboration.

CISCP hosts analyst-to-analyst technical threat exchanges and analyst training events that include government and industry partners sharing details of cyber threat activity, mitigation recommendations, and mitigation strategies. For more information, contact CISCP@us-cert.gov.

Emergency Services Sector Cybersecurity Initiative
The Emergency Services Sector (ESS) Cybersecurity Initiative is an ongoing effort to enable the ESS to better understand and manage cyber risks and to coordinate the sharing of cyber information and tools between subject matter experts (both inside and outside the federal government) and the ESS disciplines. For more information, visit https://www.dhs.gov/emergency-services-sector-cybersecurity-initiative or contact ESSTeam@hq.dhs.gov.

Emergency Services Sector-Cyber Risk Assessment (ESS-CRA). Sector-wide assessment that analyzes strategic cyber risks to ESS infrastructure. The ESS-CRA results will help the responder community understand and manage cyber risks, and provides a national-level risk profile that ESS organizations can use to prioritize how they spend resources and where to focus training, education, equipment investments, grant requests, and further study. For more information, visit https://www.dhs.gov/emergency-services-sector-cybersecurity-initiative or contact ESSTeam@hq.dhs.gov.

Emergency Services Sector Cybersecurity Framework Implementation Guidance
The Emergency Services Sector Cybersecurity Framework Implementation Guidance was developed to help Emergency Services Sector owners and operators use the voluntary Framework for Improving Critical Infrastructure Cybersecurity released by the National Institute of Standards and Technology (NIST) in 2014. For more information, visit https://www.dhs.gov/publication/ess-cybersecurity-framework-implementation-guidance or contact ESSTeam@hq.dhs.gov.

Emergency Services Sector Roadmap to Secure Voice and Data Systems The follow-up to the Emergency Services Sector-Cyber Risk Assessment (ESS-

CRA), the Emergency Services Sector Roadmap to Secure Voice and Data Systems, identifies and discusses proposed risk mitigation measures to address the risks identified in the ESS-CRA. For more information, visit https://www.dhs.gov/emergency-services-sector-cybersecurity-initiative or contact ESSTeam@hq.dhs.gov.

Enhanced Cybersecurity Services (ECS) is an intrusion prevention capability that helps U.S.-based organizations (including state, local, tribal, and territorial governments) protect their computer systems against unauthorized access, exploitation, and data exfiltration. ECS works by sharing sensitive and classified cyber threat information with accredited Commercial Service Providers (CSPs). These CSPs in turn use that information to protect customer networks from malicious activity. Groups interested in receiving ECS services and learning more about the program should visit https://www.dhs.gov/ecs or contact ECS_Program@hq.dhs.gov.

Federal Virtual Training Environment (FedVTE) is an online, on-demand training center featuring a wide range of cybersecurity courses for federal, state, local, tribal, and territorial government employees across the country. FedVTE helps users increase or maintain cybersecurity expertise and foster operational readiness at no cost. Courses range from beginner to advanced levels and are accessible from any Internet-enabled computer. For more information, visit http://niccs.us-cert.gov/training/fedvte.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). The ICS-CERT focuses on control system security across all critical infrastructure and key resource sectors. The ICS-CERT supports asset owners with reducing the risk of cyber-attacks by conducting outreach for awareness, performing assessments, providing alerts and advisories, conducting incident response activities, and performing technical analysis of malware, artifacts, and vulnerabilities. For more information, visit https://ics-cert.us-cert.gov/ or contact ICS-CERT at ics-cert@hq.dhs.gov.

If an organization believes it is experiencing a cyber event on control systems/critical infrastructure, please call 1-877-776-7585 or e-mail ICS-CERT at ics-cert@hq.dhs.gov. To report ICS software vulnerability visit http://www.kb.cert.org/vuls/html/report-a-vulnerability/ and fill out the Vulnerability Reporting Form. Please follow the directions to encrypt to the CERT Pretty Good Privacy key in order to protect sensitive, non-public vulnerability information.

Industrial Control System Cybersecurity Standards and References provide an extensive collection of cybersecurity standards and reference materials as a ready resource for the industrial control system stakeholder community. The collection provides a one-stop location for accessing papers, reports, references, and standards associated with industrial control system cybersecurity. To view the collection, visit https://ics-cert.us-cert.gov/Standards-and-References. For more information, contact ics-cert@dhq.dhs.gov.

Industrial Control Systems Cybersecurity Training. ICS-CERT performs outreach activities and assists the control systems community to improve their cybersecurity preparedness through various cybersecurity training courses. For more information, visit https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT.

Information Technology Government Coordinating Council provides a forum for interagency coordination,and partnership among DHS, National Cyber Security Division, and federal, state, local, tribal, and territorial governments with a role in protecting the IT Sector. For more information, visit https://www.dhs.gov/information-technology-sector.

Information Technology Sector Risk Assessment provides an all-hazards risk profile that public and private IT Sector partners can use to inform resource allocation for research and development and other protective measures, which enhance the security and resiliency of the critical IT Sector functions. For more information, visit www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf or contact ncsd_cips@hq.dhs.gov.

Multi-State Information Sharing and Analysis Center (MS-ISAC) seeks to improve the overall cybersecurity posture of state, local, tribal, and territorial partners. Collaboration and information sharing among members, private sector partners, and DHS are the keys to success. State, local, tribal, and territorial government representatives who believe they are experiencing a cyber event of any kind, please call 1-866-787-4722 for the 24/7 MS-ISAC Security Operations Center, or visit https://msisac.cisecurity.org/about/incidents/ and click on the "Report an Incident" button.

National Coordinating Center for Communications (NCC) continuously monitors national and international incidents and events that may impact national security and emergency preparedness communications. Incidents include not only acts of terrorism, but also natural events such as tornadoes, floods, hurricanes, and earthquakes. To receive information on the NCC or to be added to the NCC distribution list, please contact the NCC Watch at 703-235-5080 or e-mail NCC@hq.dhs.gov.

National Cybersecurity & Communications Integration Center (NCCIC) serves as a centralized location where operational elements involved in cybersecurity and communications reliance are coordinated and integrated. NCCIC partners include all federal departments and agencies; state, local, tribal, and territorial governments; the private sector; and international entities. The center's activities include providing greater understanding of cybersecurity and communications situation awareness vulnerabilities, intrusions, incidents, mitigation, and recovery actions. Stakeholders can report cybersecurity incidents (including unexplained network failures), the discovery of malicious code, and vulnerability information at https://forms.us-cert.gov/report. Contact the NCCIC Operations Center at NCCIC@us-cert.gov or 888-282-0870.

- The **Hunt and Incident Response Team (HIRT)** supports NCCIC's mission by serving as its primary operations arm, executing the asset response mission delegated to DHS in PPD-41. HIRT is the front line when responding to cyber incidents and proactively hunting for malicious cyber activity in government or private sector enterprise and industrial control systems (ICS) networks. HIRT leverages world-class expertise to lead response, containment, remediation, and asset recovery efforts with its constituents and partners. Additionally, its proactive hunt capability focuses on identifying threats from sophisticated threat actors that are often left undetected using traditional cyber security tools and techniques.

  To enable these two functions, HIRT manages, equips, and trains incident response analysts and engagement leads within an organizational culture that promotes technical excellence and dynamic mission assignments. Analysts can perform anomaly detection and trending within network traffic, analyze memory and process frequency across thousands of workstations on a network, or replicate attack activity within a sandbox environment. HIRT helps protect the Nation's key assets by preventing and mitigating advanced cyber threats through remote or onsite advanced technical assistance to Federal Government civilian

agencies and critical infrastructure asset owner operators. To learn more about HIRT's services, or to request assistance, please contact NCCICServiceDesk@hq.dhs.gov or call (888) 282-0870.

- The **National Cybersecurity & Communications Integration Center's (NCCIC) Portal,** hosted on the HSIN, is a web-based information sharing portal that enables members to exchange actionable cybersecurity information with other practitioners. NCCIC's operational branches, including the United States Computer Emergency Readiness Team (US-CERT), share cyber threat indicators, alert, and warning information, and analytical findings through structured compartments with registered public and private sector users, including state, local, tribal, and territorial government representatives. For more information and to request access, contact info@us-cert.gov.

The **National Cybersecurity Assessments and Technical Services Team (NCATS)** supports the National Cybersecurity and Communications Integration Center's mission by offering cybersecurity scanning and testing services that identify vulnerabilities within stakeholder networks and provide risk analysis reports with actionable remediation recommendations. These critical services enable proactive mitigation to exploitable risks and include network (wired and wireless) mapping and system characterization, vulnerability scanning and validation, threat identification and evaluation, social engineering, application, database, and operating system configuration review, and incident response testing. To learn more about NCATS or request information about their services, contact contactncats_info@hq.dhs.gov.

National Cyber Exercise and Planning Program (NCEPP) increases the cyber preparedness and resilience of the Nation through the conduct and development of cyber exercises and planning templates for and with public, private, and international stakeholders. As part of the National Cybersecurity and Communications Integration Center, NCEPP works with state, local, tribal, and territorial partners to provide direct cyber exercise support as a service or through participation in the Department's flagship biennial national-level cyber exercise series: "Cyber Storm." Additionally, NCEPP works with a range of stakeholders to develop and deliver planning templates, such as the Cyber Capabilities Framework and state, local, tribal, and territorial Cyber Incident Annex Template. NCEPP's cyber planning and exercise offerings are available at no cost to the state, local, tribal, and territorial community. For additional information, contact CEP@hq.dhs.gov.

National Cyber Security Awareness Month (NCSAM) is an annual campaign held each October to raise awareness about cyber security among all Americans, with law enforcement across the country participating. NCSAM, the capstone event of the nationally-known Stop.Think.Connect. Campaign, is designed to engage and educate public and private sector partners through events and initiatives with the goal of raising awareness about cybersecurity, as well as increasing the resiliency of the nation in the event of a cyber incident. The campaign works closely with members of its Cyber Awareness Coalition (comprised of federal agencies and state, local, tribal, and territorial governments) and its national network (national-level non-profit organizations). To learn more about NCSAM and find out how to get involved, contact stopthinkconnect@dhs.gov or visit https://www.dhs.gov/national-cyber-security-awareness-month.

State, Local, Tribal, and Territorial Cybersecurity Engagement Program fosters the relationships that protect our Nation's critical infrastructure and facilitates access to no-cost programs, resources, and services for state, local, tribal, and territorial governments. Governors and other appointed and elected state, local, tribal, and territorial government officials receive cybersecurity risk briefings and information on available resources. More importantly, these officials look to the program to identify cybersecurity initiatives and partnership opportunities with federal agencies, as well as state and local associations, that will help protect their citizens online. For more information, contact SLTTCyber@hq.dhs.gov.

The **Fusion Center Cyber Pilot** was a one-year pilot for developing a framework for all fusion centers on how to integrate cyber security into their area of responsibility. Under the guidance of a multi-agency review board, DHS, MS-ISAC, and others worked with six fusion centers to develop the resulting *Cyber Integration for Fusion Centers, An Appendix to the Baseline Capabilities for State and Major Urban Area Fusion Centers*. This document is accompanied by a Cyber Toolkit for fusion centers to use in building or improving their cyber programs. For more information, contact SLTTCyber@hq.dhs.gov.

The **Stop.Think.Connect. ™ Campaign** is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. Initiated by the prior Administration's Cyberspace Policy Review, DHS leads the Campaign in partnership with the National Cyber Security Alliance and the Anti-Phishing Working Group. Law enforcement agencies and other organizations can receive free cybersecurity materials (including tip sheets, presentations, and more) and collaborate with other members, including the International Association of Chiefs of Police and the Department of Justice, by joining the Cyber Awareness Coalition of government agencies or the National Network of non-profit groups. For more information, visit https://www.dhs.gov/stopthinkconnect. or contact stopthinkconnect@dhs.gov.

United States Computer Emergency Readiness Team (US-CERT) US-CERT, an incident remediation team with expertise in federal network and critical infrastructure computer security, issues alerts, bulletins, tips, and advisories to inform of threats and heighten awareness. Alerts provide timely information about current security issues, including exploits. Bulletins provide weekly summaries on newly identified vulnerabilities and include patch information, when available. Technical documents that include in-depth Internet security issues are also posted on the US-CERT website for cybersecurity practitioners.

Guidance for federal and non-federal entities to use when submitting an incident notification can be found at https://www.us-cert.gov/incident-notification-guidelines. To report an incident, malware, phishing, or vulnerabilities, visit https://www.us-cert.gov/forms/report.

US-CERT shares actionable information through its public-facing website, secure portal, and National Cyber Awareness System. Learn more about US-CERT's products and services at https://www.us-cert.gov/ and by contacting 888-282-0870 or info@us-cert.gov.

US-CERT National Cyber Awareness System (NCAS) offers subscriptions to a variety of cybersecurity information for users with varied technical expertise. NCAS products include Alerts, Bulletins, Tips, and Current Activity updates. A subscription to any or all NCAS products ensures access to timely information about security topics and threats. To learn more or subscribe, visit https://www.us-cert.gov/mailing-lists-and-feeds. This page includes information about how to use US-CERT's syndicated feeds. For additional information, contact info@us-cert.gov.

Vulnerability Notes Database and National Vulnerability Database (NVD) provide timely information about software vulnerabilities, including associated impact, solutions and workarounds, and lists of affected vendors. For more information, visit http://www.kb.cert.org/vuls, https://web.nvd.nist.gov/view/vuln/search, contact info@us-cert.gov, or call 888-282-0870.

The **Critical Infrastructure Cyber Community (C³) Voluntary Program** (pronounced "C-Cubed") is a public-private partnership aligning business enterprises, as well as federal, state, local, tribal, and territorial governments to existing resources that will assist their efforts to use the National Institute of Standards and Technology (NIST) Cybersecurity Framework to manage their cyber risks as part of an all-hazards approach to enterprise risk management. For more information, visit https://www.us-cert.gov/ccubedvp.

FEDERAL PROTECTIVE SERVICE RESOURCES

The Federal Protective Service (FPS) protects federal facilities and their occupants and visitors by providing law enforcement, protective intelligence and security services, and leveraging the information resources of a network of federal, state, local, tribal, territorial, and private sector partners. FPS provides security planning; federal facility security assessments; stakeholder engagement; law enforcement and information sharing services; and law enforcement and security incident response.

The **Explosive Detector Canine (EDC) Program** is a critical element of FPS's comprehensive security measures and supports strategic detection activities to clear identified areas of interest of explosive threats. The EDC teams provide mobile and effective capabilities for the protection of life and property through the provision of a strong, visible, and psychological deterrence against criminal and terrorist threats. EDC teams are the most effective countermeasure available today for detection of explosives. The EDC teams, each comprised of a dog and a handler with law enforcement authority, conduct searches for a variety of explosive materials on or near building exteriors, parking lots, office areas, vehicles, materials, and packages and persons in and around federal facilities. They also provide immediate and specialized response to bomb threats and unattended packages or other such dangerous items that may present a hazard to a federal facility. For more information contact the Chief of the Canine Operations Branch Uniformed Operations Division at 703-235-6080 or John.Hogan1@dhs.gov.

The **Mobile Command Vehicle (MCV) Program** supports FPS's mission through the provision of mobile, on-site platforms for command, control, and communications during terrorist attacks, natural disasters, National Special Security Events, and other similar occurrences. The MCVs can rapidly deploy to any location in the continental U.S. (and can be transported by air and sea assets if necessary) where the communications infrastructure is inadequate or has been disrupted, or where enhanced interoperability among law enforcement agencies is needed. Incident management in the nation's current threat environment requires mobility, interoperability among public safety agencies, reliability, and cost effectiveness. FPS MCVs meet this need. MCVs can support daily operations, as well as special deployments of the FPS Rapid Protection Force and other organizational elements. These highly specialized vehicles augment the capabilities of the FPS dispatch and call centers, known as MegaCenters, by allowing them to remotely dispatch units and link different radio systems together without the need to actually send personnel to the scene. Each MCV also provides an environmentally controlled platform for on-scene command and control functions, with small conferencing areas, video-teleconferencing, data

analysis and processing, and information acquisition and management for situational awareness and common operating picture development.

FPS has eight MCVs located at regional offices around the country, as well as four SUV-based mobile communications vehicles, known as "Rabbits." The Rabbits provide most of the same communications capabilities as the MCVs, but lack the command and control space and workstations. The Rabbits afford a rapid deployment capability, as well as the ability to navigate tight spaces and unimproved roads, which allows for the projection of communications services into areas that would otherwise be inaccessible. The Rabbits are designed to extend their electronic footprint into buildings of opportunity so that they can be rapidly converted into command posts with the full communications services. Strategic locations around the country ensure that each vehicle has a 750 mile "first due" response radius and that any area of the continental U.S. can be provided with service within one day. For more information, contact the Chief of the Critical Incident Management Branch, Operations Fusion Division at 703-235-6080 or scott@hq.dhs.gov.

INFRASTRUCTURE SECURITY AND RESILIENCE TRAINING AND RESOURCES

Critical Infrastructure Security and Resilience Training includes web-based independent study and classroom training and materials that address a variety of topics relevant to law enforcement that are designed to promote the knowledge and skills needed to implement critical infrastructure protection and resilience activities. The Independent Study courses developed by the Office of Infrastructure Protection are available free of charge through the FEMA Emergency Management Institute. More information about infrastructure protection training programs is available at https://www.dhs.gov/video/training-programs-infrastructure-partners.

- *Critical Infrastructure Protection: Achieving Results through Partnership and Collaboration* (IS-913) provides an overview of the elements and processes that develop and sustain successful critical infrastructure protection partnerships and collaborations. For more information, visit https://training.fema.gov/is/courseoverview.aspx?CODE=IS-913.a.
- *Implementing Critical Infrastructure Protection Programs (IS-921.a)* addresses processes for informing partnerships, sharing information, managing risk, and ensuring continuous improvement. For more information, visit https://training.fema.gov/is/courseoverview.aspx?code=IS-921.a
- *Active Shooter: What You Can Do (IS-907)* uses interactive scenarios and videos to illustrate what actions managers and employees can take when confronted with an active shooter situation, and what to expect when law enforcement arrives. For more information, visit https://training.fema.gov/is/courseoverview.aspx?code=IS-907.
- *Critical Infrastructure Security: Theft and Diversion – What You Can Do* (IS-916) is designed for critical infrastructure employees and stakeholders, and provides information and resources available to identify threats and vulnerabilities to critical infrastructure from theft and diversion of critical resources, raw materials, and products that can be used for criminal or terrorist activities. The course also identifies actions that can be taken to reduce or prevent theft and diversion. For more information, visit https://training.fema.gov/is/courseoverview.aspx?code=IS-916.
- *Protecting Critical Infrastructure Against Insider Threats (IS-915)* provides guidance to critical infrastructure employees and service providers on

how to identify and take action against insider threats to critical infrastructure. It is designed for all personnel and service providers who are associated with critical infrastructure. For more information, visit https://training.fema.gov/is/courseoverview.aspx?code=IS-915.

- *Retail Security Awareness: Understanding the Hidden Hazards (IS-912),* which is designed to make persons involved in commercial retail operations aware of the actions they can take to identify and report suspicious purchases or thefts of products that actors could use in terrorist or other criminal activities. For more information, visit https://training.fema.gov/is/courseoverview.aspx?code=IS-912.
- *Surveillance Awareness: What You Can Do* (IS-914) provides training on actions that can be taken to detect, deter, and report suspicious activities associated with adversarial surveillance. It is designed for individuals with little to no physical or operations security experience. For more information, visit http://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=is-914.
- *Workplace Security Awareness (IS-906)* which provides training for a broad audience recognizing threats and improving security in the workplace. For more information, visit http://training.fema.gov/EMIWeb/IS/IS906.asp.

These courses can be used by law enforcement to educate members of their community. The Workplace Security and Active Shooter courses are supplemented by classroom materials (instructor guides, student manuals, and visuals) that can be downloaded from the website.

Homeland Security Information Network – Critical Infrastructure (HSIN-CI) provides secure networked information sharing covering the full range of critical infrastructure interests. Validated critical infrastructure partners are eligible for HSIN-CI access. The National Infrastructure Coordinating Center (NICC) posts content from a variety of internal and external sources that is available to all critical infrastructure partners, including incident situation reports, threat reports, impact modeling and analysis, common vulnerabilities, potential indicators, and protective measures. The NICC combines current high-interest incidents and events on the HSIN-CI "front page" to enable easy access to relevant information. Individual sectors and sub-sectors self-manage more specific portals within HSIN-CI where smaller communities of participants receive and share relevant information for their particular information needs. HSIN-CI also includes capabilities to facilitate multiple types of information sharing and coordination, including suspicious activity reporting, webinars, shared calendars, etc. To ensure broad sharing of essential information, the NICC also receives and provides information via other HSIN portals. To request HSIN-CI access, submit the following to HSIN.Helpdesk@hq.dhs.gov:

- Name
- Employer
- Title
- Business email
- Brief written justification

For questions regarding HSIN-CI access, contact nicc@hq.dhs.gov or 202–282–9201.

Infrastructure Development and Recovery (IDR) Program provides infrastructure resilience planning and post-disaster recovery assistance to communities impacted by disaster. Through its infrastructure resilience planning framework and ability to leverage its network of resilience subject matter experts from across the federal interagency, academia, and other non-governmental organizations, IDR can assist communities to incorporate infrastructure security and resilience considerations throughout the infrastructure life-cycle (planning, design, operations/maintenance, and decommissioning/recovery) and across community planning

initiatives. During disaster recovery, IDR deploys infrastructure recovery experts to impacted communities who offer technical assistance and analysis to inform the prioritization of reconstitution and investment decisions, and assist with short and long-term infrastructure recovery efforts. For more information regarding the capabilities available through the IDR program, contact IDR@hq.dhs.gov.

Infrastructure Protection Gateway (IP Gateway) serves as the single interface through which DHS mission partners can access a large range of integrated IP tools and data to conduct comprehensive vulnerability assessments and data analysis. This, in turn, enables homeland security partners to quickly identify relevant vulnerability and consequence data in support of event planning and response efforts. The IP Gateway provides various data collection, analysis, and response tools into one system, streamlining access to IP's tools and datasets by leveraging a single user registration, management, and authentication process. Highlights of the IP Gateway include the ability to access:

- a selection of physical and cyber vulnerability tools and security surveys;
- a consolidated library of critical infrastructure data, assessments, and reports;
- integrated data visualization and mapping tools to support complex data analysis; and
- situational awareness tools to support special event and incident planning and response activities.

For more information, contact IPGateway@hq.dhs.gov or 1-866-844-8163.

The **National Infrastructure Coordinating Center** (NICC) serves as a clearinghouse to receive and synthesize critical infrastructure information and provide that information back to decision makers at all levels inside and outside of government to enable rapid, informed decisions in steady state, heightened alert, and during incident response. The NICC serves as the national focal point for critical infrastructure partners to obtain situational awareness and integrated actionable information to protect physical critical infrastructure. The mission of the NICC is to provide 24/7 situational awareness, information sharing, and unity of effort to ensure the protection and resilience of the Nation's critical infrastructure. When an incident or event impacting critical infrastructure occurs that requires coordination between DHS and the owners and operators of critical infrastructure, the NICC serves as a national coordination hub to support the protection and resilience of physical critical infrastructure assets. Establishing and maintaining relationships with critical infrastructure partners both within and outside the federal government is at the core of the NICC's ability to execute its functions. The NICC collaborates with federal departments and agencies and private sector partners to monitor potential, developing, and current regional and national operations of the Nation's critical infrastructure sectors. For more information, contact nicc@hq.dhs.gov or 202–282–9201.

The **Office of Cyber and Infrastructure Analysis (OCIA)** provides infrastructure consequence analysis and prioritization capabilities to DHS, government, and private sector stakeholders. OCIA experts analyze the effects of risk mitigation actions in many forms, including strategic threat and risk analysis; modeling and simulation; and analytic support to Department decision makers and security partners before, during, and after incidents. OCIA, the Office of Intelligence and Analysis, and FEMA also provide risk analysis tradecraft training to fusion centers. For access to risk analysis training contact 202-282-8866 or FusionCenterSupport@hq.dhs.gov. For questions or requests, contact OCIA@hq.dhs.gov.

Protected Critical Infrastructure Information (PCII) Program
Is it difficult to obtain the vital critical infrastructure information (CII) needed to

support critical infrastructure initiatives? Are private industry partners reluctant to share data out of fear that it could expose potentially sensitive and/or proprietary information to the public? If so, the PCII Program offers a way for homeland security analysts to access vital CII, while offering assurances to facility owners/operators that information is protected from public disclosure. Created by Congress in the Critical Infrastructure Information Act of 2002, the PCII Program ensures that PCII in the government's hands is protected from disclosure, from use in civil litigation; or for regulatory purposes. By integrating PCII protections into the data-collection process, homeland security analysts are better positioned to obtain and protect the critical business sensitive information needed to assess and understand the risk landscape, and provide leading indicators for emerging cyber security threats and vulnerabilities to critical infrastructure. To find out how the PCII Program can support your programmatic needs, contact pcii-assist@dhs.gov or at 1-866-844-8163.

Protective Security Advisors (PSAs) are security subject matter experts who engage on protective measures and resilience planning with Federal, State, local, tribal, and territorial government mission partners and members of the private sector stakeholder community to protect the Nation's critical infrastructure. As part of their mission supporting critical infrastructure protection, the PSAs plan, coordinate, and conduct security surveys and assessments; plan and conduct assistance visits; support National Special Security Events and Special Event Activity Rating events; respond to incidents; and plan, coordinate, and conduct training – to include IED awareness and IED risk mitigation training. To develop critical partnerships between the private sector and the public sector in order to mitigate risk and enhance the security of public gathering sites and special events, please visit the Hometown Security Initiative page, https://www.dhs.gov/hometown-security. For more information on these programs or to contact your local PSA, email NICC@hq.dhs.gov.

PUBLIC SAFETY AND EMERGENCY COMMUNICATIONS

All-Hazards Communications Unit Leader (COML) Course is an NPPD's Office of Emergency Communications (OEC) technical assistance course that familiarizes communications professionals with the role and responsibilities of a COML under the National Incident Management System Incident Command System (NIMS ICS) and provides exercises that reinforce the lecture materials. OEC offers this course jointly with FEMA/EMI, as "E-969, NIMS ICS All Hazards Communications Unit Leader." This course is available to state and local law enforcement agencies as part of OEC Technical Assistance. For more information, contact oec@hq.dhs.gov.

All-Hazards Communications Unit Technician (COMT) Course introduces public safety professionals and support staff to various communications concepts and technologies including interoperable communications solutions, land mobile radio (LMR) communications, and satellite, telephone, data, and computer technologies during an incident response and for planned events. The course is taught by OEC/ICTAP instructors who have both practitioner and Communications Unit experience and is designed for state, territory, tribal, and urban emergency response personnel in all disciplines who have a technical communications background. For more information, contact oec@hq.dhs.gov.

Auxiliary Communications workshop is designed for auxiliary communicators and volunteers who provide emergency backup radio communications support to public safety agencies for planned or unplanned events at state and local levels. It is designed for amateur radio operators or groups who work with public safety and cross-

disciplinary emergency response professionals. This workshop is available to state and local public safety personnel as part of OEC's Technical Assistance Program. For more information, contact oec@hq.dhs.gov.

Emergency Communications Guidance Documents and Methodologies are stakeholder-driven guidance documents and methodologies to support emergency responders across the Nation as they plan for and implement emergency communications initiatives. These resources identify and promote best practices for improving statewide governance, developing standard operating procedures, managing technology, supporting training and exercises, and encouraging use of interoperable communications. Each is available publicly and is updated as needed. Examples include the Public Safety Communications Evolution Brochure, Establishing Governance to Achieve Statewide Communications Interoperability, and the Formal Agreement and Standard Operating Procedure Template Suite. For more information, contact oec@hq.dhs.gov or visit http://www.publicsafetytools.info/.

National Emergency Communications Plan (NECP) sets goals and identifies key national priorities to enhance governance, planning, technology, and training and exercises to improve disaster communications capabilities . Originally published in 2008, the NECP was revised in 2014 to address the rapidly evolving emergency communications landscape, specifically the increased adoption of IP-based technologies. While the 2014 NECP continues to focus on the maintenance and operation of Land Mobile Radio (LMR) systems, it urges state and local jurisdictions to plan and prepare for the adoption and integration of broadband technology into emergency communications, including the Nationwide Public Safety Broadband Network (NPSBN). Continued collaboration between public and private sector entities is vital as the 2014 NECP begins to be implemented nationwide. For more information, visit https://www.dhs.gov/national-emergency-communications-plan or contact OECNECP@hq.dhs.gov.

OEC Interoperable Communications Technical Assistance (TA) Program provides technical assistance at no cost to all levels of state, local, and tribal law enforcement to support interoperable communications solutions and practices. This assistance is offered annually through Statewide Interoperability Coordinators (SWICs) based on risk and capabilities, and it supports all lanes of the SAFECOM Interoperability Continuum. There are 72 TA services offered through the OEC TA Catalog that can be viewed on the PSTools site at: http://www.publicsafetytools.info/. The services provided range from communications-focused exercises, NIMS ICS communications training to developments in broadband for public safety, dispatch operations and NG9-1-1-implementation. For more information, contact oec@hq.dhs.gov.

OEC Route Diversity Project (RDP) assists agencies on increasing the continuity of their local access networks. The local access network is the "last mile" connection between an agency's on-site communications infrastructure and the service provider's Central Office (CO) or Point of Presence (POP). In the event of an undesirable situation, such as a cable cut, flood, or damage to the service provider's facility, the local access network may be entirely lost, leaving the agency unable to perform mission-essential functions. The RDP methodologies, tools, and handbooks are designed to assist agencies in evaluating their organization's connectivity andsuggest mitigation solutions to increase route diversity. For more information, contact oec@hq.dhs.gov.

Priority Telecommunications Services (PTS) programs provide national security and emergency preparedness (NS/EP), public safety and first responders, and Critical Infrastructure Key Resources (CIKR) industries the ability to communicate on telecommunications networks during times of congestion. This is accomplished through the following three services:

- **Government Emergency Telecommunications Service** (GETS) provides priority access to the landline networks when abnormal call volumes exist, providing enhanced call completion for critical personnel.
- **Wireless Priority Service** (WPS) provides priority voice access to the cellular networks when abnormal call volumes exist, providing enhanced call completion for critical public safety personnel. An initiation fee and nominal monthly cost are associated with this service through a selected telecommunications carrier.
- **Telecommunications Service Priority** (TSP) provides priority repair and installation of critical voice and data circuits in many situations. An initiation fee and nominal monthly cost are associated with this service.

For more information, please visit the following websites: https://www.dhs.gov/government-emergency-telecommunications-service-gets; https://www.dhs.gov/wireless-priority-service-wps; and https://www.dhs.gov/telecommunications-service-priority-tsp.

The SAFECOM Program works to improve multi-jurisdictional and intergovernmental communications interoperability. Its membership includes more than 70 members representing state, local, and tribal emergency responders, and major intergovernmental and national public safety associations, who provide input on the challenges, needs, and best practices involving emergency communications. The SAFECOM website provides members of the emergency response community and other constituents with information and resources to help meet communications and interoperability needs. For more information, visit https://www.dhs.gov/safecom, or contact SAFECOMGovernance@dhs.gov.

SAFECOM Guidance on Emergency Communications Grants provides recommendations to grantees seeking funding for interoperable emergency communications projects, including allowable costs, items to consider when funding emergency communications projects, grants management best practices for emergency communications grants, and information on standards that ensure greater interoperability. The guidance is intended to ensure that federally funded investments are compatible and support national goals and objectives for improving interoperability nationwide. For more information, visit https://www.dhs.gov/safecom or contact oec@hq.dhs.gov.

The **Southwest Border Communications Working Group (SWBCWG)** serves as a forum for federal, state, local, and tribal agencies in Arizona, California, New Mexico, and Texas to share information on common issues, collaborate on existing and planned activities, and facilitate federal involvement in multi-agency projects within the Southwest Border Region. The SWBCWG aims to enhance communications operability and interoperability, effectively use the region's available critical communications infrastructure resources, and ensure that programs continue to meet the stakeholders' needs. For more information, contact oec@dhs.gov.

Statewide Communication Interoperability Plans (SCIPs) are locally driven, multi-jurisdictional, and multi-disciplinary statewide strategic plans to enhance emergency communications. The SCIP provides strategic direction and alignment for those responsible

for interoperable communications at the state, regional, local, and tribal levels. These strategic plans outline and define the current and future vision for communications interoperability within the state or territory. They also align emergency response agencies with the goals, objectives, and initiatives for achieving that vision. SCIPs are living documents that are typically updated on an annual basis, or as frequently as needed. For more information, visit https://www.dhs.gov/statewide-communication-interoperability-plans.

DHS Privacy Office (PRIV)

PRIV protects individuals by embedding and enforcing privacy protections and transparency in all DHS activities. PRIV works with every DHS component and program to ensure that privacy considerations are addressed when planning or updating any program, system, or initiative.

PRIV uses the DHS Fair Information Practice Principles as the policy framework to enhance privacy protections by assessing the nature and purpose for all personally identifiable information (PII) collected to fulfill the Department's mission.

PRIV makes much of its work publically accessible via https://www.dhs.gov/topic/privacy to share its experience and work products with DHS's partners and the public.

PRIV is always available to support state and local partnersand can be contacted at 202-343-1717 or privacy@dhs.gov.

The following materials may be of particular interest to state and local law enforcement offices, programs, and IT systems:

Privacy Compliance Reviews. PRIV issues privacy policies and conducts Privacy Impact Assessments (PIAs) to implement those policies. Later, PRIV revisits the results of these efforts to evaluate performance according to its guidance principles and standards. For more information, visit https://www.dhs.gov/investigations-reviews.

Privacy Compliance Program, Guidance, and Templates. PRIV operates a robust privacy compliance program, using the Privacy Impact Assessments (PIAs) and other tools to assess and document the integration of rules into the Department's programs and IT systems. To foster public trust through transparency, DHS publishes its PIAs, as well as the templates and guides used to create those PIAs, directly to the public. For more information, visit https://www.dhs.gov/compliance.

Policy Establishing the Fair Information Practice Principles as a Matter of Department Procedure DHS has a set of privacy principles that guide all DHS strategies, programs, and IT systems. DHS uses these principles as the foundation for new initiatives and Privacy Impact Assessments (PIAs) of existing programs. DHS memorialized these principles as department policy. For more information, visit https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

Policy Establishing the Privacy Impact Assessment (PIA) as a Standardized Government Privacy Compliance Process. PRIV uses a structured approach to build privacy protections into specific programs: DHS formally established the PIA requirement as a matter of policy. For more information, visit https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-02.pdf.

Privacy Incident Handling Guidance All organizations face the risk of privacy breaches and other incidents. PRIV created a formal approach to preparing for and responding to privacy incidents. For more information, visit https://www.dhs.gov/publication/privacy-incident-handling-guidance.

Privacy Outreach and Education PRIV shares its experience directly with the public and its partners in the public, private, and academic sectors. For more information, visit https://www.dhs.gov/privacy-events.

PRIV issues tailored educational materials to support its government and commercial colleagues, for example: The Handbook for Safeguarding Sensitive Personally Identifiable Information. For more information, visit https://www.dhs.gov/publication/handbook-safeguarding-sensitive-personally-identifiable-information

Science and Technology Directorate (S&T)

The S&T Directorate's mission is to improve homeland security by providing to customers state-of-the-art technology that helps achieve their missions. S&T customers include the operating components of the Department, and state, local, tribal, and territorial emergency responders and officials.

The Base Ensemble Personal Protective Equipment (PPE) was developed to provide new uniforms for law enforcement and other first responder agencies to wear in the performance of their daily activities and duties. These uniforms are National Fire Protection Association (NFPA) 1975 certified and provide the wearer with protection from several threats they may encounter without warning. The uniforms are flame-, splash-, and rip/tear-resistant and provide additional reinforcement at the knees, while still appearing professional. For more information, contact first.responder@hq.dhs.gov.

The **Centers of Excellence (COE)** network is an extended consortium of hundreds of universities generating ground-breaking ideas for new technologies and critical knowledge, while also relying on each other's capabilities to serve the Department's many mission needs.

Managed through S&T's Office of University Programs, the COEs organize leading experts and researchers to conduct multidisciplinary homeland security research and education. All COEs work closely with academia, industry, Department components, and first responders to develop customer-driven research solutions to 'on the ground' challenges, as well as provide essential training to the next generation of homeland security experts.

Each center is university-led or co-led in collaboration with partners from other institutions, agencies, national laboratories, think tanks, and the private sector. The research portfolio is a mix of applied research addressing both short and long-term needs. The COE extended network is also available for rapid response efforts. For more information, visit https://www.dhs.gov/science-and-technology/centers-excellence.

Datacasting Technology has been developed to address information sharing challenges faced by the public safety community. Datacasting uses the public television spectrum to allow public safety users to quickly and securely share data, including videos, images, and text that they may not be able to share using traditional networks. This provides users with reliable access to timely mission critical information from practically any location, enhancing communication and situational awareness to make informed decisions on the job. The First Responders Group conducted several successful pilots, tests, and experiments on this technology in 2015 and 2016 in Houston, TX; Chicago, IL; Washington, DC; and Boston, MA. The pilots demonstrated datacasting's ability to support public safety communications in an operational environment. Additional demonstrations are planned in 2018. Since the successful testing, datacasting has been used and will continue to be used by Houston during multiple large scale events such as the Republican Presidential Candidates' Debate, the NCAA Men's Final Four Basketball Tournament, the Chevron

Marathon, Super Bowl LV, and other incidents such as flooding due to heavy storms in the city, as well as the response to Hurricane Harvey. The First Responders Group is now working with partners on a strategy to make this technology available nationwide. For more information, contact first.responder@hq.dhs.gov.

The **Enhanced Dynamic Geo-Social Environment (EDGE) Virtual Training** provides a virtual environment platform that allows users to develop training scenarios and employ their training tactics, techniques, and procedures to respond; it also has a strategic component requiring responders to establish unified command to manage complex cross-discipline events. EDGE's three-dimensional (3-D) environment features accurate avatars, equipment, and simulations of individuals and crowds. S&T piloted its initial EDGE system with emergency response agencies in Sacramento, CA, and it is now available at no cost to response agencies nationwide. A second S&T-developed school-based active shooter capability will be available to first responders soon. Agencies will be able to customize the EDGE platform to create additional response scenarios to further meet their training needs. To learn more about simulation tools for first responders, contact first.responder@hq.dhs.gov.

The **Electronic Recovery and Access to Data (ERAD) Prepaid Card Reader** was developed for law enforcement use. The device allows law enforcement to scan and freeze prepaid cards found during an arrest or traffic stop. Prepaid cards are frequently used as financial instruments in the committing of crimes such as human trafficking and drug smuggling. The ERAD device attaches to a smartphone via the headphone port and the associated application allows for the immediate freezing and suspension of the associated assets while the proper legal process is followed to seize the funds. To protect the identities of innocent users, no user or balance information from credit or debit cards is displayed, stored, or transmitted to other locations. The card reader is available to law enforcement agencies from the ERAD Group. It is currently in operational use by state, local, and tribal law enforcement agencies and has been successfully allowing law enforcement personnel to scan suspect cards and freeze the funds on the cards for adjudication through the court system. For more information, contact first.responder@hq.dhs.gov.

Expert Tracker Training supports the U.S. Border Patrol's mission which relies on U.S. Border Patrol agents and their highly specialized skills to track and apprehend aliens and smugglers by identifying and tracking movement of personnel within a given area. Border Patrol training focused on identification of potential movement of personnel via foot traffic across borders or within unauthorized areas is standardized, but performance of tracking (i.e., sign cutting; identifying cues that indicate movement in a given area) can be vastly different. S&T developed a comprehensive, video-based training package for enhancing sign cutting perceptual and analysis skills. S&T created and transitioned 3D video training materials to the U.S. Border Patrol. For more information contact first.responder@hq.dhs.gov.

Eye-dentify/ScreenADAPT® is a visual search training platform that uses eye tracking technology to examine visual search performance in real time. ScreenADAPT®'s Eye-dentify component is a Windows based software platform that measures eye movement patterns to evaluate search performance in real time on facial images. Eye tracking is utilized while trainees examine image pairs to determine whether they match (i.e., should be cleared) or do not match (i.e., are an imposter). Students and instructors are shown immediate feedback after each image pair; they not only learn whether the student's decision was correct, but also can review the thoroughness of visual scan pattern performance on images. Eye-dentify was built as an innovative and adaptive training

module that utilizes eye tracking to capture visual search process measures in addition to behavioral responses. Eye-dentify makes the unobservable observable, allowing trainees and instructors to see how a given image pair was searched, and provides feedback on whether key features were missed. S&T transitioned twelve Eye-dentify systems to CBP in 2017. For more information, contact first.responder@hq.dhs.gov.

FirstResponder.gov is now https://www.dhs.gov/science-and-technology/first-responders. Visit the site to learn about:

- Products and standards;
- Testing and evaluation;
- Grants and training;
- Best practices;
- Opportunities for industry, academia, and the R&D community to engage with the First Responders Group (FRG).

The website features original multimedia content that highlights first responder-focused programs, initiatives, research, and events. Email first.responder@hq.dhs.gov, and engage with FRG on Facebook, LinkedIn, Twitter, YouTube, and Periscope. Or subscribe to First Responder content to receive information via email.

First Responder Communities of Practice (FR CoP) is an online network, communications and collaboration platform, sponsored by the DHS S&T, for vetted active and retired first responders; emergency response professionals; federal, state, local, tribal, and territorial Homeland Security and government officials; and academic, non-profit, and volunteers sponsored by the DHS S&T's First Responder Technologies program. Registered members of FR CoP share information, ideas, and best practices, enabling them to more efficiently and effectively prepare for all hazards. To date, First Responder Communities of Practice has more than 8,638 active members and over 218 active communities based on diverse interests and disciplines. For more information, visit https://communities.firstresponder.gov.

The **First Responders Group** is focused on fostering, through research and development (R&D), a first responder community that is connected, informed, and equipped to respond and protect the homeland. The First Responders Group identifies, validates, and helps close first responder capability gaps through existing and emerging technologies, knowledge products, and the acceleration of standards.

Projects in the First Responders Group's strategic priority areas – communications, data sharing, first responder safety and effectiveness, emerging threats (i.e., violent extremism, GPS vulnerability, unmanned aerial systems), and radiological/nuclear response and recovery research and development – result directly from close collaboration with the end users. Reflecting S&T's focus on transition, the First Responders Group has worked to ensure that technologies developed in coordination with S&T are available to first responder communities nationwide; and S&T's technologies are included in the Federal Emergency Management Agency's Authorized Equipment List (AEL) that public safety agencies are authorized to purchase from with their federal grant dollars. For more information, visit https://www.dhs.gov/science-and-technology/first-responders or email first.responder@hq.dhs.gov.

International Forum to Advance First Responder Innovation (IFAFRI)
The IFAFRI is an organization of international government leaders focused on enhancing and expanding the development of affordable, innovative technology for first responders worldwide. Representation to the IFAFRI is comprised of members from Australia, Canada, the European Commission, Finland, Germany, Israel, Japan, Mexico, The Netherlands, New Zealand, Singapore, Spain, Sweden, United Kingdom, and the United States. In the fall of 2017, S&T transitioned the

Chair of the IFAFRI to the European Commission. Following the transition, S&T is focused on achieving its goals for international engagement by increasing first responder access to innovative, affordable technology, and broadening the global first responder market for American industry. As the IFAFRI grows, it will continue to serve as a tool to discuss shared first responder capability gaps, provide a platform for collaboration on R&D initiatives and solutions, characterize global first responder markets, and educate first responders about available technology. The clearly defined list of common capability gaps, along with a true understanding of the global market will provide the international first responder community a greater voice and will help motivate industry to create advanced technologies for first responders and deliver them at affordable prices. Participating countries will have an opportunity to pool resources for addressing and resolving responder technological challenges, allowing for more R&D to be accomplished in a shorter period of time. Additionally, aggregating the user base of first responders across the globe gives new critical mass to the market. Together, IFAFRI members will help to improve the effectiveness, efficiency, and safety of first responders around the globe, resulting in improved security for all nations and citizens. To learn more, contact first.responder@hq.dhs.gov, info@internationalresponderforum.org, or visit www.internationalresponderforum.org.

The **National Urban Security Technology Laboratory (NUSTL),** located in New York City, is the only national laboratory focused exclusively on supporting state and local first responders capabilities to address the homeland security mission. The Lab provides First Responders the necessary services, products, and tools to prevent, protect against, mitigate, respond to, and recover from homeland security threats and events. NUSTL uniquely provides independent technology evaluations and assessments for first responders, thereby enabling informed acquisition and deployment decisions, and helping to ensure that responders have the best technology available to use in homeland security missions. More specifically, the Lab is mission ready to support the national first responder community by: Conducting test and evaluation of First Responder technologies and systems; advising first responders on homeland security-related technology solutions and use; and sponsoring and conducting R&D for science and technology-based solutions to respond and recover from a radiological/nuclear incident. For more information, visit https://www.dhs.gov/science-and-technology/national-urban-security-technology-laboratory or contact NUSTL@hq.dhs.gov.

The **Office of Standards,** within the Capability Development Support Group facilitates the development and integration of standards across the entire spectrum from innovation to operations. The Office works closely with federal, state, and local law enforcement partners to identify, develop, and promulgate standards through Interagency Board's Standardized Equipment List (SEL) and the FEMA Authorized Equipment List (AEL) for the law enforcement community's needs. In addition, the Office works with the National Institute of Justice (NIJ) and the National Institute of Standards and Technology (NIST) to promote the development and availability of relevant standards and associated conformity assessment programs for products and equipment listed in FEMA AEL. The Office has also entered into agreement with ASTM International to facilitate the procurement actions of the responder and law enforcement community by making standards available to state and local law enforcement and responder organizations at no cost. The Office is currently involved in developing standards for emergency response robots, personal protective equipment, urban search and rescue robots, communications equipment,

chemical and biological detectors, and others that directly address needs expressed by the law enforcement community. For more information, contact Standards@hq.dhs.gov.

The Office of Standards has commercialized Rapid DNA instruments that identify individuals and verify family relationship claims. Forensic lab processes are now available in field-ready instruments that process and analyze five DNA samples in 90 minutes. Instrument Instrument evaluations, validation samples, and accreditation protocols are available for State and local crime labs, medical examiners, and first responders.

Project 25 Compliance Assessment Program (P25 CAP) was established when S&T partnered with the Department of Commerce Public Safety Communications Research program to provide a process for ensuring that first responder communications equipment complies with P25 standards, meets performance requirements, and is capable of interoperating across manufacturers. P25 is a suite of standards that enable interoperability among digital two-way land mobile radio communications products created by and for public safety professionals, with the end goal of radios in the hands of responders that can interoperate regardless of manufacturer. P25 CAP allows emergency responders to confidently purchase and use P25-compliant products, and the program represents a critical step toward allowing responders to communicate with their own equipment. In 2009, the first eight laboratories were officially recognized by DHS as part of the P25 CAP. All equipment suppliers that participate in the P25 CAP must use DHS-recognized laboratories to conduct performance, conformance, and interoperability tests on their products. Upon completion of product testing, equipment suppliers must submit summary test reports (STR) and suppliers' declaration of compliance (SDoC) for any P25 equipment for DHS S&T review. The SDoC and STR document reviews assess the documents' completeness and accuracy in accordance with the current P25 CAP processes. For more information, visit https://www.dhs.gov/science-and-technology/p25-cap.

The **Responder Technology Alliance (RTA)** was established by the First Responders Group to reframe the discussion among first responders, the industry and investment community, and other research and development organizations to address current and future emerging technologies. The goal of the program is to leverage resources and expertise to deliver integrated responder solutions at "market speed." RTA is designed to bring a diverse set of stakeholders together to explore innovative technology solutions, standards formulation, and commercialization approaches to improve responder health, safety, and effectiveness. RTA's goal is to work with industry to change the dynamic from first responder R&D efforts that are short-term and incremental with fragmented solutions often resulting in marginal, incremental improvements to operations and interoperability, to solutions that are innovative, well integrated and make the Nation's first responders safer. To learn more, contact first.responder@hq.dhs.gov.

Response and Defeat Operations (REDOPS) program works in cooperation with the FBI's Counter-Improvised Explosive Device (IED) Unit, the National Bomb Squad Commanders Advisory Board, and state and local public safety bomb squads to enhance the Nation's ability to render IEDs safe. Through its series of test beds, REDOPS assesses emerging counter-IED technologies in areas ranging from robotics and materials handling to render-safe tools and evaluates the safety and efficacy of IED response procedures. The program's Micro R&D effort gathers innovative ideas from bomb technicians across the country, validates them and helps develop them into affordable, effective solutions that bomb squads throughout the country can implement. Several

technologies and procedures that REDOPS has evaluated are now included in the curriculum of the FBI Hazardous Devices School in Huntsville, AL, which trains and certifies all public safety bomb technicians in the United States. For more information, contact first.responder@hq.dhs.gov.

The **First Responder Resource Group (FRRG)** generates its recommendations through the Project Responder series, the most recent being Project Responder 5, published in 2017. The FRRG serves as a mechanism for continuous dialogue and the coordination of research, development, and delivery of technology solutions to first responders and the emergency preparedness and response community at the federal, state, local, tribal, and territorial levels. More than 120 responders from around the country are engaged throughout S&T's established solution development process to identify, validate, and facilitate the fulfillment of first responder needs through the use of existing and emerging technologies, knowledge products, and standards. The group meets annually in person and virtually throughout the year. The FRRG remains unique within the DHS Integrated Product Team process because its stakeholders and customers are at the state, local, tribal, and territorial levels rather than within DHS Components. Integration of first responder priorities into the overall DHS R&D budget process thus allows for the exchange of technical solutions across levels of government. To learn more, contact first.responder@hq.dhs.gov.

System Assessment and Validation for Emergency Responders (SAVER) Program assists emergency responders making procurement decisions by providing Assessment Reports, Market Surveys, TechNotes, and other types of unbiased comparative assessments of commercially available tools and equipment. The equipment is selected and then tested and evaluated by responders themselves in realistic operational environments. SAVER may also perform tests to verify manufacturer claims. SAVER reports are free to download and searchable by Authorized Equipment List (AEL) category to facilitate the need to align grant funds to AEL equipment. The goal of SAVER is to provide cost and time savings to federal, state, and local responders as they decide which equipment to purchase. The SAVER Program is managed and executed by the National Urban Security Technology Laboratory (NUSTL). SAVER documents are searchable at https://www.dhs.gov/science-and-technology/saver-documents-library. For more information, visit https://www.dhs.gov/science-and-technology/saver.

Video Quality in Public Safety (VQiPS) Working Group was formed to focus on the major policy, technology, and practical uses and challenges of public safety video systems. The working group is comprised of emergency responders across all levels of government, academia, and federal partners. In coordination with industry, the VQiPS Working Group creates knowledge products, fosters a knowledge-sharing environment, and supports research, development, testing, and evaluation for enhanced video quality through measurable, objective, and standards-based solutions across the full spectrum of video-use cases for the public safety community. For more information, contact first.responder@hq.dhs.gov.

United States Secret Service (USSS)

The mission of the Secret Service is to safeguard the nation's financial infrastructure and payment systems to preserve the integrity of the economy, and to protect national leaders, visiting heads of state and government, designated sites, and National Special Security Events.

CERT at Carnegie Mellon. In August 2000, the Secret Service and the Software Engineering Institute, a federally funded research and development

center located at Carnegie Mellon University, instituted the Secret Service CERT Liaison Program. This program positions the Secret Service to meet emerging cyber security threats as part of the agency's investigative and protective missions. The agents assigned to the CERT Liaison Program lead Secret Service-sponsored research and development, as well as direct technical support for investigative and protective operations. The agents assigned to the CERT Liaison Program work closely with the Software Engineering Institute and Carnegie Mellon University to identify and implement advanced technology in support of the full spectrum of Secret Service operations. CERT distributes forensic tools developed at the university to state and local law enforcement agencies. For more information, visit http://www.cert.org/digital-intelligence/index.cfm.

Cyber Intelligence Section (CIS) collects, analyzes, and disseminates data in support of Secret Service investigations worldwide and generates new investigative leads based upon this intelligence. CIS leverages information obtained through public and private partnerships to monitor developing technologies and trends in the financial payments industry. This information is used to enhance the Secret Service's capabilities to prevent and mitigate attacks against the financial and critical infrastructures. CIS has developed an operational investigative unit, which targets, pursues, and arrests international cyber criminals involved in cyber intrusions, identity theft, credit card fraud, bank fraud, and other computer-related crimes. CIS provides crucial information and coordination to facilitate the successful dismantling of international criminal organizations. Requests for investigative assistance should be facilitated through local Secret Service Field Offices at https://www.secretservice.gov/contact/field-offices/.

eInformation Network The Secret Service's eInformation Network is available – for free – to authorized law enforcement officers, financial institution investigators, academic partners, and commercial partners of the Secret Service. The site contains two tools: eLibrary, which allows authorized users to obtain credit card issuing bank information; and U.S. Dollars Counterfeit Note Search, a site that provides the user with the ability to conduct a search of the Secret Service counterfeit note database. For more information, visit www.einformation.usss.gov

Electronic Crimes Special Agent Program (ECSAP) ECSAP-trained special agents conduct forensic examinations of computers, mobile devices, and other electronic media. These agents possess the knowledge, training, and expertise to collect and process digital evidence to support computer-related investigations in the field. They provide support and expertise in the investigations of network intrusions, Point of Sale (POS), Business Email Compromises (BEC), Ransomware, and other database thefts. The program establishes and maintains relationships with the private sector in order to continually improve its knowledge of emerging trends, tactics, and techniques prevalent in the cybercriminal world. The ECSAP program can be a crucial resource for federal, state, and local law enforcement partners. USSS examiners have assisted partner agencies and departments in financial crime, violent crime, and child exploitation investigations. USSS agents can conduct forensic examinations for other federal, state, or local law enforcement upon request. For more information, please contact the local Secret Service Field Office at https://www.secretservice.gov/contact/field-offices/.

Electronic Crimes Task Force (ECTF). The USA PATRIOT Act of 2001 mandated the Secret Service to establish nationwide Electronic Crimes Task Forces to combine the resources of academia; the private sector; and local, state, and federal law enforcement agencies for the purpose of *"preventing, detecting, and investigating various forms of electronic crimes, including*

potential terrorist attacks against critical infrastructure and financial payment systems." There are currently 40 Secret Service ECTFs, to include London, England and Rome, Italy. Membership in the Secret Service ECTFs includes approximately 350 academic partners; over 3,100 international, federal, state, and local law enforcement partners; and over 4,000 private sector partners.

Financial Crimes Enforcement Network (FinCEN), a bureau within the Department of Treasury, provides financial transaction information to law enforcement at the federal, state, local, and international level. FinCEN enhances the integrity of financial systems by facilitating the detection and deterrence of financial crime, by receiving and maintaining financial transactions data; analyzing and disseminating that data for law enforcement purposes; and building global cooperation with counterpart organizations in other countries and with international bodies. FinCEN utilizes numerous databases to provide intelligence and analytical support to law enforcement investigators protecting the U.S. financial system from the abuses of criminal activities to include terrorist financing, money laundering, and other illicit activity. For more information, please contact the local Secret Service Field Office at http://www.secretservice.gov/contact/field-offices/.

Financial Crimes Task Forces (FCTF) Through years of collaboration on investigative endeavors, the Secret Service has established unique partnerships with state, local, and other federal law enforcement agencies. Leveraging those partnerships with the agency's long-standing cooperation with the private sector, the Secret Service has established a national network of Financial Crimes Task Forces (FCTFs). The FCTFs combine the resources of the private sector with those of diverse law enforcement agencies in an organized effort to combat threats to the nation's financial payment systems and critical infrastructures. These task forces are well-suited to conduct complex, in-depth, multi-jurisdictional investigations. Through membership in a FCTF, local and state law enforcement entities gain access to a variety of investigative resources including FinCEN, INTERPOL, and IOC-2 databases. For more information, please contact the local Secret Service Field Office at http://www.secretservice.gov/contact/field-offices/.

International Organized Crime Intelligence and Operations Center (IOC-2) The U.S. Department of Justice's IOC-2 marshals the resources and information of nine U.S. law enforcement agencies, as well as federal prosecutors, to collectively combat the threats posed by international criminal organizations to domestic safety and security. The Secret Service IOC-2 detailee serves as the liaison between the Secret Service and the IOC-2 acting as a conduit for information and requests in support of field agents. For more information, please contact the local Secret Service Field Office at http://www.secretservice.gov/contact/field-offices/.

Mobile Device Forensic Facility The Mobile Device Forensic Facility in Tulsa, OK was created in 2008 to meet the challenges associated with the forensic extraction of data from mobile devices. The Secret Service established a partnership with the University of Tulsa, Digital Forensic Laboratory Center of Information Security to create and co-locate the Mobile Device Forensic Facility at the University. The facility provides training and conducts forensic examinations and research on mobile devices. The ongoing research into these new devices, operating systems, and mobile device technologies provides valuable tools in the Secret Service's fight against cybercrime. Requests for investigative assistance should be facilitated through the local Secret Service Field Office at https://www.secretservice.gov/contact/field-offices/.

National Center for Missing and Exploited Children The

Secret Service supports the National Center for Missing and Exploited Children (NCMEC) and local law enforcement with its expertise in forensic analysis to include crime scene, handwriting, document authentication, ink analysis, fingerprints and photography, graphic design, video productions, audio and image enhancement, and speaker recognition services. Specialized polygraph and crime scene services are evaluated upon request. The Secret Service also offers two community outreach programs that are delivered to schools and communities across the nation. "Operation Safe Kids" provides parents with a document containing biographical data, a current photograph, and digitized inkless fingerprints. In the event a child who participates in this initiative is ever reported as missing, lost, or abducted, his/her fingerprints can be retrieved from the parents. The Childhood Smart Program is a joint partnership with NCMEC, in which the Secret Service assists NCMEC with their "Kidsmartz" and "Netsmartz" programs, which heighten awareness regarding child safety issues. Educational resources include topics such as child pornography, online enticement, child sex tourism, commercial sexual exploitation, and child abduction. The initiative focuses on delivering age appropriate real world and Internet safety presentations to children in various settings, which include classrooms, recreational camps, and community events, etc. For more information, visit https://www.secretservice.gov/contact/field-offices/ and https://www.secretservice.gov/investigation/.

National Computer Forensics Institute (NCFI) – Hoover, AL. The NCFI was established in 2007 through a partnership initiative between DHS, the Secret Service, and the Alabama District Attorneys Association. The NCFI offers state and local law enforcement officers, prosecutors, and judges a variety of cyber-related training courses based on the Secret Service electronic crimes training model. NCFI offers the following 15 courses: Basic Investigation of Computer and Electronic Crimes Program, Basic Scripting Techniques, Basic Computer Evidence Recovery Training, Advanced Forensics Training, Basic Network Investigation Training, Network Intrusion Response Program, Basic Mac Investigation Training, Basic Mobile Device Investigations, Mobile Device Examiner, Advance Mobile Device Examiner, Online Social Networking, Computer Forensics in Court – Prosecutors, Computer Forensics in Court – Judges, Mobile Devices in Court – Prosecutors and Mac Forensics Training. NCFI provides funding for all travel expenses, as well as hotel and per diem for state and local law enforcement officers. Additionally, all NCFI graduates receive hardware, software, and licenses necessary to conduct forensic computer and network intrusion examinations. For more information, visit www.ncfi.usss.gov.

Transportation Security Administration (TSA)

TSA protects the nation's transportation systems to ensure freedom of movement for people and commerce.

Assistant Federal Security Directors for Law Enforcement (AFSDs-LE) The AFSD-LE, working under the direction of the Federal Security Director (FSD), works to establish and maintain liaison with local, state, and federal law enforcement authorities, as well as coordinate activities taking place within their assigned transportation domain, on behalf of TSA's Office of Law Enforcement/Federal Air Marshal Service.

Typical liaison contacts for the AFSDs-LE may include airport police authority, Transportation Security Officers, ICE, the Joint Terrorism Task Force, CBP, the TSA Office of Inspection, and any other local, state, and/or federal agencies whose investigative interests may have a nexus to the transportation system within TSA's area of responsibility. For more

information on TSA's AFSD-LE program, visit www.tsa.gov or contact your OLE/FAMS Supervisory Air Marshal in Charge (SAC) or FSD.

Commercial Vehicle Counter-Terrorism Training Created under commission by TSA, the DHS Federal Law Enforcement Training Centers (FLETC) worked directly with state, federal, and municipal law enforcement agencies to identify the most effective ways for on-site officers to identify and intercept commercial vehicle-borne terrorist threats. Training at FLETC facilities or to law enforcement units at home stations has been certified as eligible for DHS reimbursement through state assistance programs. Visit the FLETC website for more information: https://www.fletc.gov/training-program/commercial-vehicle-counterterrorism-training-program or contact the FLETC Glynco office at 912-267-3587.

Counter-Terrorist Guides Pocket-sized publications directed to surface transportation providers in highway, mass transit, passenger and freight rail, and pipeline modes identify terrorist techniques, motivation, and opportunities to disrupt potential threats. These colorful guides have become many of the TSA Surface Division's most popular publications. For more information visit https://www.tsa.gov/for-industry/surface-transportation or contact TSA-Surface@tsa.dhs.gov.

First Observer Plus™ Domain Awareness Training. Available online at TSA.gov, training modules speak directly to transportation professionals to enhance their understanding of terrorist techniques and threats, providing a message of "Observe, Assess, Report." Modules are available for highway-related professions, individuals working in mass transit and passenger rail, over-the-road bus, school bus, general trucking and parking, trucking hazardous materials, trucking food and agriculture, truck rental, and parking for large venues and mass gatherings. Tens of thousands of civilian transportation workers have been trained to date, and TSA's domain awareness programs have been directly credited with disrupting terrorist events. To learn more, contact FirstObserver@tsa.dhs.gov or visit https://www.tsa.gov/for-industry/firstobserver.

Intermodal Security Training and Exercise Program (I-STEP) provides exercise, training, and security planning tools and services to the transportation community. I-STEP is the only federal exercise program to focus on the security nexus of the intermodal transportation environment. As a result, it not only reduces risk to individual systems, but the entire transportation network. Working in partnership with the various transportation modes, I-STEP provides a variety of products and services that enable security partners to enhance security capabilities by participating in and conducting exercises and training that strengthens security plans, tests emergency procedures, and sharpens skills in incident management. I-STEP builds partnerships by collaborating with modal partners, law enforcement personnel and other first responders, medical professionals, government leaders, and industry representatives to address challenges in transportation security. For more information, contact 571-227-5150 or ISTEP@dhs.gov.

- Managed by the I-STEP, the **Exercise Information System (EXIS)** is the only exercise tool specifically tailored to the transportation sector. EXIS takes a step-by-step approach as it guides users though exercise planning. First, it directs users to identify the exercise planning schedule and sector focus; next it enables users to select specific objectives and scenario elements; and finally, it allows users to plan evaluation criteria, share best practices and lessons-learned, and create post-exercise reports. EXIS communities facilitate information sharing among users. Users can create private communities and

sub-communities to design operator-specific exercises and to delegate tasks to other planning team members. EXIS is provided at no cost by the TSA as an integral part of I-STEP. To become an EXIS member, visit https://exis.tsa.dhs.gov/default.aspx. For more information, contact EXIS@dhs.gov.

Insider Threat Program (ITP) is managed by the OLE/FAMS, Security Services and Assessments Division (SSAD), Security Assessments Section (SAS). The mission of the Insider Threat Unit (ITU) is to deter, detect, and mitigate an insider from causing harm to the Nation's transportation domain. To accomplish this mission, ITU responsibilities include Training and Awareness Outreach; Operations-Referrals and Mitigation; and Insider Threat Assessments in coordination with TSA's Office of Security Operations. To address insider threats, the ITU coordinates inquiries and investigations with the appropriate lead entities (internal and external stakeholders) to include TSA offices; federal, state, and local law enforcement; as well as various airport and transit agency/commuter rail law enforcement agencies.
For more information, contact: InsiderThreat@tsa.dhs.gov.

Joint Vulnerability Assessment (JVA) Program In accordance with 49 U.S.C. § 44904, the SAS, under the OLE/FAMS, SSAD, performs non-regulatory JVAs of physical security at U.S. airports. The primary focus of the JVA is to identifiy vulnerabilities that are above and beyond Federal Regulation compliance that may directly impact the aviation domain. A final comprehensive report is presented to the Federal Security Director with mitigation options. JVAs are a joint effort undertaken by the TSA and FBI with the purpose of assessing current and potential threats to commercial air transportation facilities within the United States. The FBI submits a threat assessment under a separate cover.

In addition, JVA collaborates with the TSA Office of Security Operations to provide airports with a Self-Vulnerability Assessment Tool for yearly self-testing; and also provides FSDs a JVA Recognized Practices Guide that summarizes common areas of vulnerabilities and provides suggested mitigation strategies, some of which are no or low cost utilizing existing TSA resources. This guidebook may be made available to airport authorities and associated law enforcement entities upon request. For more information, contact OLEFAMSSAS@tsa.dhs.gov.

Law Enforcement Officer (LEO) Reimbursement Program Provides partial reimbursement to state, local, or other public institutions or organizations responsible for commercial airport operations within their jurisdiction, as specified in U.S. statute or TSA program guidance documents and regulations. Funding is intended to help defray the cost of providing highly visible law enforcement presence and support of passenger screening activities at U.S. commercial airports. For more information, contact LEO.Reimbursements@dhs.gov.

Man-Portable Air Defense Systems (MANPADS) Awareness Program. MANPADS are portable surface to air guided missile systems designed to be carried by an individual. The SAS, under the OLE/FAMS, SSAD, conducts MANPADS Vulnerability Assessments (MVA) at commercial airports nationwide in an effort to identify and define potential launch areas, areas that are rated on the basis of seven specific characteristics. A multi-dimensional approach is designed to detect, deter, and defeat a MANPADS threat against civil aviation. SAS also provides oversight and guidance on the development and implementation of MANPADS mitigation plans at the commercial airports.

SAS provides a MVA Basic Training Program (MVABTP) course that provides field personnel with the basics on how to conduct a MVA and the

requirements for the MMP (MANPADS Mitigation Plans). In addition, it will provide knowledge on how to identify areas of concern for other stand-off weapons threats. Report templates, reference, and briefing material will be provided to all trainees.

SAS provides MANPADS awareness training and outreach to local law enforcement and other first responders. The Law Enforcement MANPADS Awareness Training Program (LEMATP) provides law enforcement and other first responders with the basic knowledge on how to mitigate an attack. The course includes MANPADS capabilities, SAS MVA methodology and selection of sites, the requirements for a MMP, patrol/security techniques, law enforcement response to a MANPADS attack, and investigative tips after a MANPADS attack. TSA also provides MANPADS pocket identification cards and posters to law enforcement and first responders to assist in the identification of MANPADS and their components.
For more information, contact OLEFAMSSAS@tsa.dhs.gov.

Sensitive Security Information (SSI) Program
SSI is information obtained or developed which, if released publicly, would be detrimental to transportation security, and is defined at 49 CFR Part 1520. SSI is not authorized for public disclosure and is subject to handling and safeguarding restrictions.

The TSA SSI Program, the central SSI authority for all of DHS, develops SSI guidance and training materials to assist state and local law enforcement partners in the recognition and safeguarding of SSI. The SSI Program also develops SSI policies and procedures, analyzes and reviews records for SSI content, and coordinates with stakeholders, other government agencies, and Congress on SSI-related issues.

For more information about SSI or for assistance in identifying SSI, visit https://www.tsa.gov/for-industry/sensitive-security-information or contact 571-227-3513 or SSI@tsa.dhs.gov.

The **TSA Contact Center (TCC)** is responsible for fielding incident reports from the public. TSA's Internal Affairs Division (IAD) is responsible for conducting criminal and administrative investigations of employees who are alleged to have committed misconduct, including identifying and investigating potential worker's compensation fraud by TSA employees. If a person suspects that a TSA employee is engaging in misconduct or fraud, they are asked to contact TSAInspectionHotline@tsa.dhs.gov and provide the name of the employee suspected of alleged misconduct and an explanation of the issue, including date(s) and time(s). They also are asked to provide their name and contact information for appropriate follow-up. Employees should provide their name even if they choose to remain anonymous throughout the process. The public also may report security-related incidents to TCC, and may request follow up information on the status of those reports through TCC.

TSA Law Enforcement Officer (LEO) Flying Armed Training Program. The TSA Office of Training and Development, Training Centers Division is responsible for oversight of the TSA LEO Flying Armed Training Program, which is *mandatory* for all law enforcement officers flying armed under the Code of Federal Regulation 1544.219, Carriage of Accessible Weapons. The LEO Flying Armed training is a 1.5 to 2 hour block of instruction that is comprised of a structured lesson plan, slide presentation, FAQs, NLETS procedures, and applicable codes of Federal regulation. This material is provided to federal, state, local, territorial, tribal, and approved railroad law enforcement agencies and departments to properly instruct their officers on the subject of flying on board commercial aircraft while armed. The training includes protocols in the handling of prohibited items, prisoner transport, and dealing with an act of criminal violence aboard an aircraft. The program

training materials may be requested on TSA's website, https://www.tsa.gov/travel/law-enforcement. The request will be sent to the TSA Office of Training and Development, Training Centers Division. Questions regarding the LEOFA training materials may be sent to LEOFA_TRN@tsa.dhs.gov from an agency email address.

To receive this training material you must:

- Be a full-time law enforcement officer meeting the instructor qualification standards of the agency, academy, or department in which you are employed;
- Select/click the "Request Training Materials" tab on the TSA website and requested information will be prompted through a fillable form, then include the following: (1) Name and contact information (enter an agency email address); (2) Department's name and address; (3) Supervisor's name and contact information; (4) A brief narrative detailing operational need to fly armed; and (5) additional information for processing purposes.

If you are not a qualified instructor, please request a member of your training staff to contact us by email. For time sensitive training requests, please call (855) FLY-LEOS between the core business hours of 8:00 am to 4:00 pm EST. If directed to voicemail, please leave a detailed message with your contact information.

Visible Intermodal Prevention and Response (VIPR) Program Focused on deterrence and detection of terrorist activities, TSA VIPR operations promote confidence in and protect our nation's transportation systems through the targeted deployment of integrated assets utilizing law enforcement and screening capabilities in coordinated activities to augment security in any mode of transportation. VIPR teams may deploy Federal Air Marshals and other TSA security capabilities, including explosive trace detection and Preventative Radiological/Nuclear Detection technologies. The Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS) administers the VIPR Program and uses a risk-based concept of operations to assist with program management, as well as to ensure an element of randomness and unpredictability in operations. These VIPR operations are conducted in all modes of aviation and surface transportation. Teams also may be deployed to provide an additional law enforcement or security presence at transportation venues during specific alert periods or in support of special events.

For more information on TSA's VIPR resources, visit www.tsa.gov or contact your local OLE/FAMS SAC or FSD.

APPENDIX A - ACRONYMS

ACAMS	Automated Critical Asset Management System
AEL	Authorized Equipment List
AMOC	Air and Marine Operations Center
ANSI	American National Standard Institute
BCOT	Building Communities of Trust
BCSC	National Bulk Cash Smuggling Center
BEST	Border Enforcement Security Task Force
BMAP	Bomb-making Material Awareness Program
BPA	Blanket Purchase Agreement
BSC	Biometric Support Center
C3	Cyber Crime Center
CAB	Community Awareness Briefing
CAP	Criminal Alien Program
CBP	U.S. Customs and Border Protection
CBRNE	Chemical, Biological, Radiological, Nuclear and Enhanced Conventional Weapons
CCU	Cyber Crimes Unit
CDF	Capability Development Framework
CDM	Continuous Diagnostics and Mitigation
CDP	Center for Domestic Preparedness
CEIU	Child Exploitation Investigation Unit
CERT	Computer Emergency Response Team
CFATS	Chemical Facility Anti-Terrorism Standards
CFU	Computer Forensics Unit
CGMIX	USCG Maritime Information eXchange
CI	Critical Infrastructure
CIFW	Counterintelligence Fundamental Workshop
CIPD	Counterintelligence Division
CIS	Cyber Intelligence Section
CMaaS	Continuous Monitoring as a Service
COE	Centers of Excellence
COI	Community(ies) of Interest
COML	Communications Unit Leader
COMT	Communications Unit Technician
COP	Common Operating Picture
CP	Continued Presence
CPAA	Cultural Property, Art, and Antiquities
CRCL	Office for Civil Rights and Civil Liberties
CRR	Cyber Resiliency Review
CSEP	Cybersecurity Evaluation Program
CVE	Countering Violent Extremism
CVEC	Countering Violent Extremism Coordinator
DARTTS	Data Analysis & Research for Trade Transparency Systems
DBFTF	Document and Benefit Fraud Task Force
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DHS-SPS	DHS Single Point of Service
DMV	Department of Motor Vehicles
DNDO	Domestic Nuclear Detention Office
DOE	Department of Energy
DOJ	Department of Justice
DOS	Department of State
DSF	Deployable Special Forces
ECSAP	Electronic Crimes Special Agent Program
ECTF	Electronic Crimes Task Force
EDCT	Explosive Detection Canine Team
EDD	Explosive Detector Dog
EDGE	Enhanced Dynamic Geo-Social Environment
EMI	Emergency Management Institute
EOC	Emergency Operations Center
ERO	ICE Enforcement and Removal Operations
ESS	Emergency Sector Services
ESS-CRA	Emergency Sector Services-Cyber Risk Assessment
EXIS	Exercise Information System
FAA	Federal Aviation Administration
FAR	Fugitive Alien Removal
FBI	Federal Bureau of Investigation
FCTF	Financial Crimes Task Force
FDNS	Fraud Detection and National Security
FEDSIM	Federal Systems Integration and Management Center
FEMA	Federal Emergency Management Agency
FinCEN	Financial Crimes Enforcement Network
FiRST	First Responder Support Tool
FLETC	Federal Law Enforcement Training Centers
FOT	Fugitive Operations Teams
FOUO	For Official Use Only
FPS	Federal Protective Services
FRG	First Responders Group
FRRG	First Responder Resource Group
FR CoP	First Responder Communities of Practice
FSCC	Federal Sponsored Course Catalog
FSLTT	Federal, State, Local, Tribal, Territorial
FY	Fiscal Year
GNDA	Global Nuclear Detection Architecture
GPD	Grant Programs Directorate
GPS	Global Position System
GSA	General Services Administration
HAZMAT	Hazardous Materials
HME	Homemade Explosives
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
HSDN	Homeland Security Data Network
HSI	ICE Homeland Security Investigations
HSIN	Homeland Security Information Network
I&A	Office of Intelligence and Analysis
IAB	Interagency Board
IAD	Internal Affairs Division
IAQ	Immigration Alien Query
IC	Intelligence Community
IED	Improvised Explosive Device
IEEE	Institute of Electrical and Electronics Engineers
ICE	U.S. Immigration and Customs Enforcement

ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ICTAP	OEC Interoperable Communications Technical Assistance Program
IDENT	Automated Biometric Identification System
IMAGE	ICE Mutual Agreement between Government and Employers
IMPACT	Incident Management Preparedness and Coordination Toolkit
INTERPOL	International Criminal Police Organization
IOC-2	International Organized Crime Intelligence and Operations Center
IP	Intellectual Property
IPAWS	Integrated Public Alert and Warning System
IPR	Intellectual Property Rights
IPR Center	National Intellectual Property Rights Coordination Center
I-STEP	Intermodal Security Training and Exercise Program
ISIL	Islamic State of Iraq and the Levant
ITA	Intelligence Training Academy
JAC	Joint Analysis Center
JACCIS	JAC Collaborative Information System
JACTAWS	Joint Counterterrorism Awareness Workshop Series
JVA	Joint Vulnerability Assessment
LEO	Law Enforcement Officer
LESC	ICE Law Enforcement Support Center
LEISI	Law Enforcement Information Sharing Initiative
LEIS Service	Law Enforcement Information Sharing Service
LEMATP	Law Enforcement MANPADS Awareness Training Program
LES	Law Enforcement Sensitive
LESC	Law Enforcement Support Center
LMR	Land Mobile Radio
LMS	Learning Management System
MANPADS	Man-Portable Air Defense Systems
MCV	Mobile Command Vehicle
MDDP	Mobile Detection Deployment Program
MDDU	Mobile Detection Deployment Unit
MISLE	Marine Information for Safety and Law Enforcement
MJIEDSP	Multi-Jurisdictional Improvised Explosive Device Security Planning
MS-ISAC	Multi-State Information Sharing Center
MVA	MANPADS Vulnerability Assessments
MVABTP	MANPADS Vulnerability Assessments Basic Training Program
NBIC	National Biosurveillance Integration Center
NCAS	National Cyber Awareness System
NCATS	National Cybersecurity Assessment and Technical Services Teams
NCC	National Coordination Center
NCCAD	National Counter-IED Capabilities Analysis Database
NCCIC	National Cybersecurity and Communications Integration Center
NCEPP	National Cyber Exercise and Planning Program
NCFI	National Computer Forensics Institute
NCSAM	National Cybersecurity Awareness Month
NCTC	National Counterterrorism Center
NECP	National Emergency Communications Plan
NEDCTP	National Explosives Detection Canine Team Program
NFOP	National Fugitive Operations Program
NGI	Next Generation Identification
NGO	Nongovernmental Organization
NICC	National Infrastructure Coordination Center
NIMS	National Incident Management System
NIMS ICS	NIMS Incident Command System
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NPPD	National Protection and Program Directorate
NPSBN	Nationwide Public Safety Broadband Network
NSI	Nationwide Suspicious Activity Reporting (SAR) Initiative
NTAS	National Terrorism Advisory System
NTED	National Training and Education Division
NUSTL	National Urban Security Technology Laboratory
OBIM	Office of Biometric Identity Management
OBP	Office of Bombing Prevention
OCIA	Office of Cyber and Infrastructure Analysis
OCSTF	Operation Community Shield Task Forces
ODLS	Online Detainee Locator System
OEC	Office of Emergency Communications
OHA	Office of Health Affairs
OIG	Office of Inspector General
OSLLE	Office for State and Local Law Enforcement
OSLTC	ICE Office of State, Local, and Tribal Coordination
OTPP	Office for Terrorism Prevention Partnerships
P25 CAP	Project 25 Compliance Assessment Program
PED	USCIS Public Engagement Division
PERC	Pacific Enforcement Response Center
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PLEPU	Parole and Law Enforcement Programs Unit
PM	Program Management
PPE	Personal Protective Equipment
PRIV	DHS Office of Privacy
PRND	Preventative Radiological/Nuclear Detection
PRD	Personal Radiation Detector
PSA	Protective Security Advisors
R&D	Research and Development
RAAS	Report Analysis and Archive System
RD	Regional Directors
REDOPS	Response and Defeat Operations
RFI	Request for Information
RKB	Response Knowledge Base

RIID	Radiation Isotope Identification Device
RISS	Regional Information Sharing System
R/N	Radiological and Nuclear
RTA	Responder Technology Alliance
S&T	Science and Technology Directorate
SAS	Security Assessment Section
SAVER	System Assessment and Validation for Emergeny Responders
SBU	Sensitive but Unclassified
SCIP	Statewide Communication Interoperability Plan
SDOC	Suppliers Declaration of Compliance
SEL	Standard Equipment List
SEVP	Student Exchange Visitor Program
SLT	CBP State, Local, Tribal, Liaison
SLTD	State, Local, and Tribal Division
SLTT	State, local, tribal, and territorial
SPBP	Significant Public Benefit Parole
SSI	Sensitive Security Information
STC	Securing the Cities
STR	Summary Test Report
SWBCWG	Southwest Border Communications Working Grp.
SWIC	Statewide Interoperability Coordinator
TA	Technical Assistance
TBML	Trade-Based Money Laundering
TCC	TSA Contact Center
TCO	Transnational Criminal Organization
TRIP*wire*	Technical Resource for Incident Prevention
TSA	Transportation Security Administration
TTU	Trade Transparency Unit
UASI	Urban Area Security Initiative
US-CERT	U.S. Computer Emergency Readiness Team
USCG	U.S. Coast Guard
USCIS	U.S. Citizenship and Immigration Services
USSS	United States Secret Service
VAP	Victims Assistance Program
VAWA	Violence Against Women Act
VBIED	Vehicle-borne Improvised Explosive Device
VIG	Vehicle Inspection Guide
VIPR	Visible Intermodal Prevention and Response Program
VQiPS	Video Quality in Public Safety
VWP	Visa Waiver Program
WMD	Weapons of Mass Destruction

APPENDIX B - INDEX