DHS State and Local Law Enforcement Resource Catalog

Volume IV

February 2016

U.S. Department of Homeland Security

Intentional Blank Page. Please Continue to Next Page.

Letter from the Office for State and Local Law Enforcement

March 1, 2016

Dear Law Enforcement Partners:

Homeland security begins with hometown security, and DHS tirelessly works to get tools, information, and resources out of Washington, D.C. and into the hands of our state, local, and tribal law enforcement partners. With the release of the *DHS State and Local Law Enforcement Resource Catalog Volume III*, we are pleased to announce a continuation of that effort.

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 across the Department to our law enforcement partners.

At DHS, we are continually developing new programs and resources that could be of assistance to state, local, and tribal 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 has always worked to enhance the support that DHS provides to our law enforcement partners. We hope this catalog is another one of those tools that will assist in your efforts to keep our communities safe, secure, and resilient.

Sincerely,

Office for State and Local Law Enforcement
Department of Homeland Security

Office for State and Local Law Enforcement

Overview

On the recommendation of the 9/11 Commission, Congress created the Office for State and Local Law Enforcement (OSLLE) in 2007 to lead the coordination of DHS-wide policies related to state, local, tribal, and territorial 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 the 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 www.dhs.gov/active-shooter-preparedness. Materials are also 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 fundalmental/basic skills;
- _Active Shooter Threat Instructor Training Program (ASTITP)_ – instructor level, "train-the-trainor" program;
- _Basic Tactical Medical Training Program (BTMTP)_ – provide skills to enhance the law enforcement

officer's ability to provide emergency first aid for traumatic and non-traumatic injuries during an active threat scenario; 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 which are needed to successfully serve as a law enforcement first responder in an active shooter/threat situation. 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.   To learn more about FLETC training courses available to state, local, and tribal law enforcement and for contact information, visit https://www.fletc.gov/state-local-tribal or contact stateandlocaltraining@dhs.gov.

Within the Homeland Security Information Network (HSIN), the Joint DHS and FBI Countering Violent Extremism (CVE) and Active Shooter 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 firemen and EMS), 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:

1. Full Name;
2. Place of Employment;
3. Job Title;
4. Work Email Address;
5. Work Phone Number;
6. 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 protect the basic right of freedom and to bring those who exploit human lives to justice. Increased awareness and training will lead to more tips to law enforcement, which results in more victims being identified. We cannot do this alone so please join us in the fight to end human trafficking. Visit the Blue Campaign website to learn about how we can work together and to find out about available training, outreach materials, and victim assistance. To learn more, visit www.dhs.gov/bluecampaign

or, contact BlueCampaign@hq.dhs.gov.

You can also 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 provide a benefit to law enforcement;
- Scenario based videos depicting indicators of sex trafficking and labor trafficking;
- Printed educational and reference materials for law enforcement, non-governmental organizations, judicial officials, first responders, school staff, and victims or potential victims; and
- Human trafficking awareness posters and public service announcements.

To access these and other products, visit www.dhs.gov/bluecampaign.

Common Operating Picture (COP) is a suite of capabilities that provides government and private sector Homeland Security Enterprise professionals with enhanced situational awareness to facilitate 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 identify courses of action during an event or threat situation. The DHS COP provides users a broad set of capabilities based on best-in-class technologies that deliver a rich, end user experience through a web-accessible interface.

The DHS COP is an application that supports the DHS mission of responding to threats and hazards to the nation by collecting, sharing, and displaying multi-dimensional information that facilitates collaborative planning and responses to these threats. For more information, contact GMO@hq.dhs.gov.

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

Tripwire. HSIN is made up of 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, to 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 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 New York's 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 www.dhs.gov/ifyouseesomethingsaysomething.

National Terrorism Advisory System (NTAS) has replaced the Homeland Security Advisory System as our 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 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 will secure America's promise as a nation

of immigrants by providing accurate and useful information to our customers, granting immigration and citizenship benefits, promoting an awareness and understanding of citizenship, and ensuring the integrity of our immigration system. Read the full mission statement at www.uscis.gov/aboutus.

Avoid Scams is a webpage for the public to find information about how to recognize and report immigration scams and the unauthorized practice of immigration law, and how to find authorized help with immigration services. To learn more, visit www.uscis.gov/avoidscams, or www.uscis.gov/eviteestafas in Spanish.

Fraud Detection and National Security (FDNS) Units. USCIS Field Operations Directorate FDNS Units are staffed with immigration officers, who are well-versed in immigration related fraud and national security issues. Immigration officers not only assist in the adjudications 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. Immigraiton 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 60 immigration officers in the JTTF Program, and 25 immigraiton officers in most of the 21 ICE-led DBFTFs. In addition, designated immigration officers in all 26 District Offices have made positive contact with a point-of-contact at state and local fusio ncenters, usually the DHS I&A representative. For more information, please contact USCISFODFDNSOps@uscis.dhs.gov.

Law Enforcement Support Operation Unit. USCIS's Fraud Detection and National Security (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," 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 http://www.uscis.gov/green-card/other-ways-get-green-card/green-card-informant-s-nonimmigrant.

USCIS's 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 www.uscis.gov or contact Public.Engagement@dhs.gov.

USCIS Resources is a webpage with links to a variety of publications and other materials for USCIS customers, the organizations that serve them, and the public. Visit www.uscis.gov/resources.

USCIS provides the latest version of its applications and petitions on its website. All forms are free and available at 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 Form I-918, Petition for U Nonimmigrant Status, and T visa applicants may submit a law enforcement certification with their Form I-914, Application for T Nonimmigrant Status. The investigating or prosecuting law enforcement agency does not apply to USCIS for a T or U visa on the victim's behalf. The victim applies to USCIS T and U visa and USCIS reviews the request and all submitted evidence to determine eligibility. Related resources include:

- The **U and T Visa Law Enforcement Resource Guide** provides law enforcement officials information about U and T visa requirements, the law enforcement certification process, and answers to frequently asked questions from law enforcement agencies to support investigations and prosecutions involving immigrant victims of human trafficking and other crimes. Included in the guide is a selection of best practices and a frequently asked questions section that draws upon questions received by state and local law enforcement. The guide is available electronically at http://www.dhs.gov/publicat ion/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 www.uscis.gov/tools/resour ces/information-law-enforcement-agencies-and-judges. For law enforcement inquiries, contact LawEnforcement_UTVAW A.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, contact USCIS at T_U_VAWATraining@usci s.dhs.gov.

Citizenship and Immigration Services Ombudsman (Ombudsman's Office)

The Ombudsman's Office is available to help law enforcement with issues or concerns that they have regarding their interactions with USCIS. The Ombudsman's Office is an independent, impartial, and confidential office within DHS 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 Ombudsman's Office. The 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 Ombudsman's Office. 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 of the request for assistance. For more information, see 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 right 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; and the Rehabilitation Act of 1973, as amended.

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, and related statutes. Information for recipients on meeting their nondiscrimination requirements under Title VI is available on CRCL's website, www.dhs.gov/title-vi-overview-recipients-dhs-financial-assistance.

CRCL 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 (www.dhs.gov/guidance-published-help-department-supported-organizations-provide-meaningful-access-people-limited). For more information, please contact crcl@hq.dhs.gov.

Common Muslim American Head Coverings and Common Sikh American Head Coverings Posters provide 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 14 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 www.dhs.gov/civil-rights-and-civil-liberties-institute.

CRCL Impact Assessments review Department programs, policies, and activities to determine whether these initiatives have an impact on the civil rights and civil liberties of those affected by the initiative. For more information about CRCL Impact Assessments, visit www.dhs.gov/crcl.

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 which 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

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 http://www.dhs.gov/publication/crcl-newsletter.

Guidance Regarding Use of Race for Law Enforcement Officers. Developed by CRCL in partnership with the Department of Justice (DOJ), this training reviews the DOJ guidance regarding racial profiling.
Duration: 20 minutes. CD-ROMs can be ordered from CRCL by emailing crcltraining@hq.dhs.gov.

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 www.dhs.gov/crcl.

Introduction to Arab American and Muslim American Cultures is an hour-long training DVD, released in the fall of 2006, that provides insights from four national and international experts, including an Assistant U.S. Attorney who is a practicing Muslim; a member of the National Security Council who is a practicing Muslim; a scholar of Islamic studies; and a civil rights attorney who advocates on issues of concern to Arab American and Muslim American communities. The training assists law enforcement officers and other personnel who interact with Arab and Muslim Americans, as well as individuals from Arab or Muslim communities in the course of their duties. For more information, visit http://www.dhs.gov/civil-rights-and-civil-liberties-institute or contact crcltraining@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 and sheriffs 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 Limited English Proficiency plans that many sheriff's offices have put in place to meet the requirements of Title VI of the Civil Rights Act. 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, samples, or customization of a low literacy version, email crcltraining@hq.dhs.gov.

Privacy, Civil Rights & Civil Liberties Fusion Center Training Program. The Implementing Recommendations of the 9/11 Commission Act requires 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 & Analysis and the

DOJ Bureau of Justice Assistance to deliver this training program. The program has included: A website resource center 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 your procedures); privacy fundamentals (how to integrate your 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. Technical assistance is also available.
Duration: Full-day (eight hours) but can be customized to shorter sessions. For more information, email FusionCenterTraining@hq.dhs.gov.

The First Three to Five Seconds: Arab and Muslim Cultural Awareness for Law Enforcement. This course is intended to help law enforcement personnel to better understand the culture of Arab and Muslim Americans, including topics such as why an individual's name may differ among documents and general background on Islam in the United States. This video was developed by the DOJ Community Relations Service and reproduced by DHS. *Duration*: 10 minutes.

For more information, visit www.dhs.gov/civil-rights-and-civil-liberties-institute. This site also offers a transcript and limited resources and glossary. You may order DVDs from CRCL by emailing crcltraining@hq.dhs.gov.

Web Portal for Privacy and Civil Rights & 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.

Available at: 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 larger 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 basically any commissioned USCG vessel 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, most commonly recognized and widely utilized are National Security Cutters, High and Medium Endurance Cutters (420-foot, 378-foot, 270-foot,

and 210-foot) and our smaller 87-foot Marine Protector Class,110-foot Island Class, and 154-foot Sentinel Class patrol vessels.

There are a total of 190 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 and C-144 Ocean Sentry turboprops) operate from large and small Air Stations. Rotary wing aircraft (H-65 Dolphin and HH-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 (11), Port Security Units (8), Tactical Law Enforcement Teams (2), Maritime Security Response Team (1), National Strike Force and Regional Dive Lockers (2). 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 Boardings; 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 Position System (GPS) augmentation signals that permit high-precision

positioning and navigation. For more information, visit http://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
Baltimore	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	904-564-7511
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	251-411-6211
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	415-399-3300
San Juan	San Juan, PR	787-289-2041
Sault Ste. Marie	Sault Ste. Marie, MI	906-632-0967
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 Community Partnerships (OCP)

DHS has relaunched its Countering Violent Extremism (CVE) public webpage in 2014 and it will undergo further revision this year. On the webpage, individuals can find information about the Department's approach and resources such as a CVE tool-kit, information on "Building Communities of Trust", and information on how to apply for access to the DHS-FBI CVE Training Resources and Active Shooter Webportal. The webpage is further being updated with resources and relevant links. You can access the Department's CVE landing page at:
http://www.dhs.gov/topic/countering-violent-extremism#.

Enhanced Engagement and Training Resources.
The Community Awareness Briefings (CAB)
To enhance engagement efforts and provide awareness training in regards to CVE, DHS, in partnership with the National Counterterrorism Center (NCTC), developed and is delivering the CAB. This briefing has been conducted in cities across the country to communities and state, local, and federal law enforcement.

The CAB is designed to share unclassified information regarding the threat of violent extremism. The CAB has been conducted in 14 U.S. cities over the past few years. It is designed to help communities and law enforcement develop the necessary understanding of al-Qa'ida, al-Shabaab, Islamic State of Iraq and the Levant (ISIL), and related affiliates' recruitment tactics and explore ways to collectively and holistically address these threats before they become a challenge at the local level. Due to the increased number of Western-based fighters traveling to foreign war conflicts, such as Syria and Somalia, the CAB now includes information relating to the foreign fighter recruitment narrative by al Shabaab and ISIL, and the myths versus realities of the situation in Syria and Somalia.

To learn more about the CAB please email:
OSLLE@hq.dhs.gov.

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.

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. Border Community Liaisons nationwide can be assessed through the CBP State, Local, Tribal Liaison Office at 202-325-0775 or by emailing CBP-STATE-LOCAL-TRIBAL-LIAISON@cbp.dhs.gov.

CBP Information Center provides general information about CBP requirements and procedures, as well as handling the intake for complaints related to CBP interactions. The CBP INFO Center also maintains an on-line database of Q&A's covering all aspects of customs and immigration operations. The CBP INFO Center can be reached at 877-CBP-5511 or 202-325-8000 or by visiting https://help.cbp.gov/app/home.

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 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 http://cbp.gov/xp/cgov/toolbox/contacts/ports/.

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 www.cbp.gov/xp/cgov/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 http://cbp.gov/xp/cgov/toolbox/contacts/ports/.

Preventing International Non-Custodial Parental Child Abduction. DHS 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. If you are concerned about the international travel of a child, please contact the DOS Office of Children's Issues at PreventAbduction@state.gov or the 24 hour hotline 888-407-4747.

State, Local and Tribal Liaison. A component of the CBP Commissioner's Office, the State, Local, and Tribal Liaison strives to build and maintain effective relationships with state, local, and tribal governments through regular, transparent, and proactive communication. Governmental questions regarding issues and policy pertaining to border security, trade, and facilitation can be referred to the SLT at CBP-STATE-LOCAL-TRIBAL-LIAISON@cbp.dhs.gov or 202-325-0775.

Suspicious Aircraft or Boats. The CBP Air and Marine Operations Center (AMOC) is responsible for securing the airspace at and beyond our 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.

Domestic Nuclear Detection Office (DNDO)

DNDO is a jointly staffed office within DHS. DNDO is the primary entity in the U.S. government for implementing domestic radiological and nuclear (R/N) detection efforts for a managed and coordinated response to R/N threats, as well as integration of federal nuclear forensics programs. DNDO is charged with coordinating the development of the global nuclear detection and reporting architecture, with partners from federal, state, local, tribal, territorial, and international governments and the private sector. For more information, visit www.dhs.gov/about-domestic-nuclear-detection-office or contact DNDO.INFO@hq.dhs.gov.

Equipment Test Results. Federal, state, local, tribal, and territorial agencies intending to purchase 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. DNDO has

resources that are available to assist federal, state, local, tribal, and territorial entities in selecting the right R/N detection equipment to meet their operational needs.

DNDO has conducted several equipment test campaigns to evaluate the effectiveness of detection systems in multiple performance areas to better support R/N detection procurement decisions and concept of operations development by federal, state, local, tribal, and territorial stakeholders.

These test campaigns have included detection system categories such as: radiation isotope identification devices (RIIDs), personal radiation detectors (PRDs), backpacks, and mobile systems (vehicle-mounted, boat-mounted, and aerial-mounted).

When test reports are completed and are available for release, federal, state, local, tribal, and territorial stakeholders are notified via DNDO Operations Support Directorate's weekly newsletter, *The Source*. To be added to the distribution list for *The Source*, simply email a request to DNDO.JAC2@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 DNDO stakeholders related to the radiological detection mission. For more information contact the DMAMC at DMAMC@hq.dhs.gov

The GRaDER® Program. GRaDER® provides objective and reliable performance testing information to federal, state, and local 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 www.dhs.gov/GRaDER or email GRaDER.questions@hq.dhs.gov.

Joint Analysis Center (JAC). The JAC, located within DNDO, provides awareness of the Global Nuclear Detection Architecture (GNDA) and provides technical support to federal, state, local, tribal, and territorial authorities. Utilizing the Joint Analysis Center Collaborative Information System (JACCIS), the JAC facilitates R/N alarm adjudication from detection events and consolidates and shares information and databases.

GNDA Awareness is achieved by establishing and maintaining links to detectors and access to Nuclear Regulatory Commission and Agreement State Material Licensing Data. GNDA Awareness also depends

upon non-time critical requirements such as access to historical data on all detection events (illicit and legitimate) and access to information about commerce and related R/N infrastructure that affects detection assets and response protocols.

JACCIS provides federal, state, local, tribal, and territorial stakeholders adjudication connectivity, a detector database, and status information regarding the events and activities relating to R/N detection and nuclear forensics at the "Unclassified//For Official Use Only" level. In this capacity, JACCIS maintains awareness of the GNDA, which involves facilitating alarm adjudication and monitoring global efforts in R/N detection. JACCIS is completely web enabled so connectivity is possible anywhere in the country in real-time and utilizes an agile development process to release updates every quarter. The JAC provides information integration and analysis coupled with awareness of the GNDA. This enables the right information to be available at the point of detection and ensures that detection events result in either a proper response to a threat or a quick dismissal of a non-threat. To contact the JAC, call 866-789-8304 or e-mail DNDO.JAC2@hq.dhs.gov. For more information, visit www.dhs.gov/about-domestic-nuclear-detection-office.

Mobile Detection Deployment Units (MDDU).
Collaboration between federal, state, local, tribal, and territorial law enforcement and public safety agencies is crucial to a layered approach to radiological and nuclear security. DNDO developed the MDDU as a surge asset to assist federal, state, local, tribal, and territorial agencies detect and report radiological and nuclear threats. The MDDU was designed to supplement radiological and nuclear detection capabilities in support of national and special security events, or in response to an intelligence-driven event.

MDDUs are mobile trailer packages containing radiation detection equipment for up to 40 public safety professionals. MDDU packages are prepositioned across the United States and are maintained and deployed for DNDO by U.S. Department of Energy (DOE) Radiological Assistance Program (RAP) personnel. The equipment includes personal radiation detection devices, 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 DOE RAP technical support staff to train federal, state, local, tribal, and territorial personnel on the use of the specific MDDU equipment, and to help

integrate these capabilities into existing operations.

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

Open Access to American National Standards Institute (ANSI) N42 Series Standards. DNDO sponsors the Institute of Electrical and Electronics Engineers (IEEE) to provide 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/.

Radiological and Nuclear Detection Exercises. DNDO's Exercises Program provides support in developing, designing, and conducting discussion or operational-based R/N detection exercises that are compliant with the Homeland Security Exercise and Evaluation Program methodology. Exercises provide valuable hands-on experience for federal, state, and local personnel performing R/N detection missions and assist decision makers in integrating the R/N detection mission into their daily operations. Additional information about R/N detection exercises is available by contacting DNDO at

DNDO.SLA@hq.dhs.gov.

Radiological /Nuclear Detection and Adjudication Capability Development Framework (CDF). The Capability Development Framework (CDF) provides guidance to federal, state, local, tribal, and territorial stakeholders to assist jurisdictions in identifying and developing recommended levels of R/N detection capability based on risk factors and the likelihood of encountering illicit R/N material. The CDF informs stakeholders of potential gaps in their ability to detect, report, and respond to R/N material outside of regulatory control. It is intended to provide strategic guidance based on best practices, but not to establish specific requirements. The CDF is a DNDO product that supports the Screening, Search, and Detection Core Capability and can be leveraged to support investment justifications. A CDF Calculator is also available to assist jurisdictions with identifying recommended levels of R/N detection capability quickly and easily. The CDF and supporting resources are available on the Homeland Security Information Network (HSIN) PRND Community of Interest (COI) web portal or by contacting DNDO.SLA@hq.dhs.gov.

Radiological/Nuclear Detection National Incident Management System (NIMS) Resource Types. DNDO

coordinated the development of R/N detection resource types in partnership with federal, state, local, tribal, and territorial subject matter experts to support planning and organization, and increases efficiency and effectiveness for sharing R/N detection resources through the Emergency Management Assistance Compact and other mutual aid mechanisms. The NIMS-typed teams, equipment, and job titles provide a common categorization of R/N detection resources. FEMA is currently conducting a review to include these as national level tier one resources. The latest resource type definitions can be obtained by contacting DNDO.SLA@hq.dhs.gov.

Radiological and Nuclear Detection Community of Interest (COI). DNDO's R/N Detection COI is a site located on the Homeland Security Information Network (HSIN) that provides a repository of useful information on DNDO, PRND, the Global Nuclear Detection Architecture (GNDA), 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 DNDO with a message subject line of: "DNDO RND COI HSIN Access Request" to the address: PRND_COI@hq.dhs.gov.

Radiological and Nuclear Detection Assistance Program. DNDO works with federal, state, local, tribal, and territorial government policy makers, program managers, and operational administrators to design, implement, and sustain a R/N detection program. DNDO's R/N Detection Assistance Program includes the development of concepts of operation, standard operating procedures, multiyear Training and Exercise Plans, Sustainment Plans, table top exercises (coordinated through the Exercises Program), and the sharing of lessons learned and best practices.

The program goal is to prevent the use of an R/N terrorist weapon against the interior or maritime portion of the United States. The Assistance Program seeks to establish sustainable R/N Detection capabilities among federal, state, local, tribal, and territorial agencies and emergency responders to detect and report unauthorized R/N materials out of regulatory

control within their jurisdictions/regions. To request assistance or for more information on DNDO's Assistance Program, contact DNDO.SLA@hq.dhs.gov

Radiological and Nuclear Detection Training. DNDO's Training Program provides quality products to support, develop, enhance and expand R/N detection capabilities in support of the GNDA. Together with other federal partners, the DNDO Training Program provides instructional courses in basic, intermediate, advanced, and train-the-trainer R/N detection tactics, techniques, and procedures. The DNDO 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 federal, state, local, tribal, and territorial agencies 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. DNDO and its partners have completed R/N detection training for over 35,000 law enforcement, first responder personnel, and public officials through Fiscal Year 2015.

R/N detection training courses are available through FEMA's

National Preparedness Directorate. Courses are taught by the National Domestic Preparedness Consortium member: Counter-Terrorism Operations Support (CTOS) – Center for Radiological/Nuclear Training. For more information, visit www.ctosnnsa.org/. Courses are also available through the FEMA Federal Sponsored Course catalog. FEMA FSCC Web page: www.firstrespondertraining.gov/webforms/pdfs/fed_catalog.pdf. For additional information regarding R/N detection training, visit https://gnda.energy.gov or email DNDO.SLA@hq.dhs.gov.

Securing the Cities (STC) Program. The STC Program assists state, local, and tribal stakeholders design and implement or enhance existing architectures for coordinated and integrated detection and interdiction of nuclear materials out of regulatory control that may be used as a weapon within high-threat/high-density Urban Area Security Initiative (UASI) areas. Urban Areas selected through a competitive application process. The program assists these jurisdictions by using cooperative agreements to enhance regional capabilities to detect, identify, and interdict nuclear materials that are out of regulatory control, guide the coordination of federal, state, local, and tribal entities in their roles defined by the GNDA and encourage participants to

sustain their nuclear detection program over time. There are three phases to the program. In Phase I, STC assists state and locals in developing an initial operating capability to detect and report the presence of nuclear materials that are out of regulatory control. The initial regional capabilities are mutually supportive through cooperative agreements, region specific operations, interoperable equipment, collective training, and progressive exercise planning. In Phase II, STC provides additional resources to enhance detection, analysis, communication, and coordination to better integrate state and local capabilities with Federal government activities and the GNDA beyond Phase I. Finally, in Phase III, STC provides indirect support to sustain the program. DNDO works with regional partners to maintain connectivity with the established local architecture through alarm adjudication and subject matter expertise and provides advice on long-term training, exercise, and other program support. State and local participants will maintain and continue to improve their developed capabilities to support the GNDA using local funds or other Federal Government grant funds. For more information, email DNDOSTC@hq.dhs.gov.

Federal Emergency Management Agency (FEMA)

FEMA's mission is to support our citizens and first responders to ensure that as a nation we work together to build, sustain, and improve our 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 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 speak to 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 four guides designed for Houses of Worship, Institutions of Higher Education, Schools for Kindergarten through Twelfth Grade, U.S. Airports, and Medical Care Facilities. For more information and for electronic copies of the guides visit, www.fema.gov/plan.

The **Authorized Equipment List (AEL)**, published and maintained by the FEMA Grant Programs Directorate (GPD), is a tool used by grantees 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 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 which allows grantees to search for items by keyword, equipment category, or item number. Each item page includes the specific grant program(s) for which the item is allowable; a description of the item; and SEL data including operating considerations, item standards, and training information. For more information visit: http://beta.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. An electronic version of the guide is available at http://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 the diverse responder disciplines: Emergency Management, Emergency Medical Services, Fire Service, Governmental Administrative, Hazardous Materials, Healthcare, Law Enforcement, Public Health, Public Safety Communications, and Public Works.

- 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.

- 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, non-governmental and private sector, and the whole community.

- National Training and Education Division (NTED) serves the nation's first responder community, offering more than 150 courses to help build critical skills that responders need to function effectively in mass consequence events. NTED 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 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 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.

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 more than 16 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 and 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 and competitive grants to enhance the capacity of state, local, tribal, territorial, and private sector emergency responders to prevent, protect against, respond to, and recover from 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 www.fema.gov/preparedness-non-disaster-grants or 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 communications systems. [Continuity of Operations]() is an effort within departments and agencies to ensure that Primary Mission Essential Functions continue to be performed during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies.

- 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 level 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 at IPAWS@fema.dhs.gov.

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, and tribal 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, and tribal 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, and tribal law enforcement and for contact information visit https://www.fletc.gov/state-local-tribal or contact stateandlocaltraining@dhs.gov.

The **FLETC Online Campus** is a secure online Academic Learning Management System (ALMS) developed by the FLETC in support of the law enforcement learning environment. The Online Campus currently offers over 100 professionally developed interactive online courses that are available for U.S. sworn and vetted law enforcement officers and agents. The Online Campus registration and access to course materials is provided through the Regional Information Sharing System (RISS), law enforcement officers and agents are required to complete the RISS Automated Trusted Information Exchange Application™ (ATIX) applicaiton. For more information, visit www.fletc.gov/e-fletc-online-campus.

Office of Health Affairs (OHA)

OHA serves as DHS's principal authority for all medical and health issues. OHA provides medical, public health, and scientific expertise in support of the DHS mission to prepare for, respond to, and recover from all threats. OHA serves as the principal advisor to the Secretary and the Federal Emergency Management Agency (FEMA) Administrator on medical and public health issues. OHA leads the Department's workforce health protection and medical oversight activities. The office also leads and coordinates the Department's biological and chemical defense activities and provides medical and scientific expertise to support the Department's preparedness and response efforts.

OHA has four strategic goals that coincide with the strategic goals of the Department:

- Provide expert health and medical advice to DHS leadership;
- Build national resilience against health incidents;
- Enhance national and DHS medical first responder capabilities; and
- Protect the DHS workforce against health threats.

For more information on OHA resources for support to state and local law enforcement, please send an e-mail to HealthAffairs@dhs.gov, or NOC.OHA@hq.dhs.gov.

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. OHA 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 OHA 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 electronically at http://www.dhs.gov/publication/iedactive-shooter-guidance-first-responders.

The **National Biosurveillance Integration Center (NBIC)** integrates biosurveillance activities across the human health, animal, plant, food, water, and environmental domains to provide a biological common operating picture and facilitate earlier detection of adverse events and trends. NBIC works in partnership with federal, state, local, territorial, tribal, 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 are available on the Homeland Security Information Network (HSIN) to public health, health care, agriculture, environment, and law enforcement personnel across the country at all levels of government. To request access to HSIN-NBIC-SL, contact nbicoha@hq.dhs.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 ICEEnforcement and Removal Operations (ERO).

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 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 abuse, and white collar crime. VAP also provides information to victims on post-correctional release 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 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 combated 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 our 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.

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. Additional information on CAP may be found at 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. More information on the NFOP can be found at www.ice.gov/fugitive-operations and http://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 wants and 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 Commaactind 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 with a state or local law enforcement agency on a part-time basis or in a full-time capacity. More information on the Joint Effort Initiative can be found at www.ice.gov/fugitive-operations.

Law Enforcement Information Sharing Initiative (LEISI) facilitates the sharing of DHS sensitive but unclassified law enforcement information with other federal, tribal, state, local, and international law enforcement 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 LEISI at 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 that 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 an automated biometric (fingerprints) submission or a biographic, 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 www.ice.gov/lesc.

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.

The **Priority Enforcement Program (PEP)** focuses on individuals convicted of significant criminal offenses or who otherwise pose a threat to public safety, such as gang members. Under PEP, ICE will only seek transfer of individuals in state and local custody in specific, limited circumstances. ICE will only issue a detainer where an individual fits within DHS's narrower enforcement priorities and ICE has probable cause that the individual is removable. In many cases, rather than issue a detainer, ICE will instead request notification (at least 48 hours, if possible) of when an individual is to be released. ICE will use this time to determine whether there is probable cause to conclude that the individual is removable and arrange for the safe and orderly transfer of the criminal alien from the state or local law enforcement agency. Additional information on PEP may be found at https://www.ice.gov/pep.

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 locate and arrest criminal and other priority aliens who pose a threat to our nation's communities. By leveraging technology and partnerships with domestic and international law enforcement, regulatory, and intelligence agencies, the NCATC provides a specialized law enforcement workforce that analyzes the nature and characteristics of the removable alien population. The NCATC, in coordination with other ICE ERO and ICE enforcement entities, serves as an operational component of ICE's cooperative and community safety-based concept.

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 www.ice.gov/fugitive-operations.

Online Detainee Locator System (ODLS) is a public system available online at www.ice.gov 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 come. 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.

ICE HOMELAND SECURITY INVESTIGATIONS (HSI)

Border Enforcement Security Task Force (BEST). In response to a significant increase in violence along the Southwest border, ICE HSI, in partnership with U.S. Customs and Border Protection (CBP), as well as other federal, state, local, tribal, territorial, and international law enforcement officials have expanded its ongoing Border Crimes Initiative by creating BEST, a multi-agency initiative. To date, a total of 37 BESTs have been initiated across 16 states and in Puerto Rico. These teams are comprised of over 1,000 members who represent over 100 law enforcement agencies that have jointly committed to investigate transnational criminal activity along the Southwest Border, Northern Border, and at our nation's major seaports. For more information, visit www.ice.gov/best/.

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 http://www.ice.gov/cultural-art-investigations. Reports may be sent to HSIculturalproperty@ice.dhs.gov.

Cyber Crimes Center (C3), a component of ICE HSI, was established in 1997 for the purpose of combating crimes committed on, or facilitated by, the Internet. C3 is ICE HSI's main focal point for coordinating the agency's cyber strategy as it relates to cybercrime and computer forensics. ICE HSI's main 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 provide 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 http://www.ice.gov/cyber-crimes/.

Document and Benefit Fraud Task Forces (DBFTF). ICE HSI leads 23 interagency task forces 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, Harlingen, Houston, Honolulu, Los Angeles, Miami, New York, Newark, Orlando, Philadelphia, Sacramento, Salt Lake City, San Francisco, San Juan, St. Paul, 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 is the ICE HSI Forensic Laboratory, and the ICE HSI Cyber Crimes Center (C3). For more information, visit www.ice.gov/document-benefit-fraud/.

Forced Labor Program. ICE HSI investigates allegations of forced labor in violation of the Tariff Act of 1930 (Title 19 USC §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.

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, please email the Identity and Benefit Fraud Unit at ibfu-ice-hq@dhs.gov.

ICE HSI Forensic Laboratory (HSI-FL) provides a broad range of 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 Society of Crime Laboratory Directors / Laboratory Accreditation Board (ASCLD/LAB). Forensic disciplines include questioned documents, fingerprints, and chemistry. 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 www.ice.gov/hsi-fl.

ICE HSI International Operations Overseas Offices represent DHS' 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 to increase foreign capacity through outreach and training.

To locate and contact any of the ICE HSI International Offices, go to

http://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, 365 days per 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 www.ice.gov/tips.

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 http://www.ice.gov/human-rights-violators-war-crimes-unit.

The Department of Homeland Security (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 information regarding human smuggling. HSC will provide a means to operationalize intelligence in a timely manner to identify and disrupt human smuggling organizations. HSC is committed to a collaborative approach to detect, deter, disrupt and dismantle current human smuggling network activity, to include those organizations engaged in the movement of Central Americans and unaccompanied children to the United States. Defined by its function as a human smuggling targeting mechanism, the DHS/HSC will have access to the entire spectrum of human smuggling intelligence and will fuse this information into timely, operationalized intelligence products designed to enhance field enforcement efforts.

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 our borders, during traffic interdictions, and other law enforcement encounters. The BCSC targets transnational criminal organizations who 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 our 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 Federal Bureau of Investigation (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.

These task forces enable the IPR Center to leverage the resources, skills, and authorities of each partner, and they provide a comprehensive response to intellectual property theft. For additional information on available training opportunities, please contact the IPR Center at IPRCenter@dhs.gov. For more information on the IPR Center, visit http://www.iprcenter.gov/.

Operation Community Shield is the ICE HSI anti-gang initiative that combines 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 our federal, state, local, tribal, and foreign law enforcement partners. With our partners, ICE HSI enhances intelligence gathering and information sharing, exploits 21st century law enforcement technology, and capitalizes on our 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 http://www.ice.gov/national-

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) serves as the clearinghouse for all Significant Public Benefit Parole (SPBP) applications to ICE from federal, state, and local law enforcement agencies. SPBP is a mechanism that allows otherwise inadmissible aliens to come to the United States for law enforcement purposes.   For more information on the SPBP program, please call 800-973-2867.

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.

Additionally, 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 www.ice.gov/news/library/facts heets/shadow-wolves.htm.

Title 19 Cross-Designation. Title 19 of the U.S. Code section 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 Title 19 U.S.C. § 1401(i) harness their invaluable experience with this unique federal authority to collectively enhance joint investigations of narcotics smuggling, money laundering, and fraud-related activities that 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 Narcotics, Smuggling, and BEST Unit in Washington, D.C., or email the unit at HSITFO@ice.dhs.gov.   For additional information, visit 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 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 IE—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 placement 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.

Building Communities of Trust (BCOT). The BCOT initiative focuses on developing trust among law enforcement, fusion centers, and the communities they serve to address the challenges of crime and terrorism prevention. Since initial implementation, the BCOT initiative has been administered primarily by the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI), a program that provides law enforcement with a capacity for gathering, documenting, processing, analyzing, and sharing suspicious activity reports

about behaviors that have a potential nexus to terrorism. The NSI recognizes that each community has an important role in preventing crime and terrorism and uses the concept of community policing to build trust and cooperation to share information with state, local, tribal, and territorial law enforcement officers.

To help ensure that appropriate SAR reporting takes place, it is essential that law enforcement and community members have strong, trusting relationships. As these relationships are developed and maintained, members of the community are more likely to report crime and suspicious activities, which is why the NSI has worked with partners at the federal, state, and local levels—including U.S. Attorneys' Offices, privacy advocacy groups, faith leaders, and a diverse group of local community members—to implement the BCOT initiative.

The BCOT initiative has been implemented in over 15 urban areas across the country, with roundtables hosted by police chiefs, sheriffs' departments, and fusion centers through the support of U.S. Attorneys, Federal Bureau of Investigation field office executives, fusion center directors, and DHS field representatives.

Community leaders and local law enforcement share responsibility for addressing the prevention of crime and

terrorism in their neighborhoods. BCOT roundtables provide a forum for community leaders and law enforcement officials to have a candid conversation on how to work together to keep communities safe from terrorism, crime, violence, and other locally-based problems that would be better

solved together. For more information, visit http://www.dhs.gov/publication/building-communities-trust-bcot-initiative, or contact your local Fusion Center.

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 will be 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 Homeland Security Information Network (HSIN). To access or sign-up for HSIN, visit http://www.dhs.gov/homeland-security-information-network-hsin

DHS-Single Point of Service (DHS-SPS) serves as DHS Headquarter' central ingest point for receiving, tracking, and facilitating Operational and Intelligence Requests For Information (RFIs) to and from federal, state, local, tribal, and territorial partners. This process—undertaken by I&A and the Office of Operations Coordination and Planning—is not a replacement for existing lines of communication; rather, it serves as a resource to facilitate validated RFIs with an organization capable of providing a response. Before

submitting an RFI to SPS, Federal and DHS Component partners should route their RFIs through their respective headquarters to ensure they have visibility. State and local partners should work through their Fusion Center(s) (via their deployed I&A Staff) to verify all local resources have been exhausted.

DHS-SPS representatives can be contacted at:

Open/STE: 202-282-9555
NSTS: 766-0888

NIPR: DHS-SPS-RFI@dhs.gov
HSDN: DHS-SPS-RFI@dhs.sgov.gov
JWICS: DHS-SPS-RFI@dhs.ic.gov.

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. To assist in the development of this capability, the U.S. Department of Homeland Security (DHS) and the U.S. Department of Justice (DOJ) partnered in 2007 to offer a series of fusion center technical assistance services. These services have been developed based on the input and guidance from the DHS

Office of Intelligence and Analysis (I&A); the Office of the Director of National Intelligence (ODNI); the Office of the Program Manager, Information Sharing Environment (PM-ISE); the Federal Bureau of Investigation (FBI); and experts from the state and local community— including the Global Justice Information Sharing Initiative (Global), the Criminal Intelligence Coordinating Council (CICC)—and will be delivered by subject-matter experts with experience in the development and operation of fusion centers. Fourteen services are offered to support the implementation of the *Fusion Center Guidelines,* the *Information Sharing Environment* (ISE) *Implementation Plan*, and the *Baseline Capabilities for State and Major Urban Area Fusion Centers* to facilitate the nationwide development and/or enhancement of the fusion process. To learn more or to apply for assistance please visit: https://ncirc.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) coordinates the design and delivery of entry, mid-level, and advanced intelligence training for I&A, the DHS Intelligence Enterprise (IE), and state, local, territorial, and tribal partners throughout the United States. The mission of the ITA is to advance students' knowledge, skills, and abilities through the creation and dissemination of homeland security intelligence training. The ITA is located in Washington, D.C. To obtain a copy of the ITA's course catalog or training calendar, please contact the IA-Registrar@hq.dhs.gov.

The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI). The NSI was established to facilitate 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://nsi.ncirc.

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, visit http://www.dhs.gov/bombing-prevention-training. To request

training, contact your local Protective Security Advisor (PSA) or contact OBP@hq.dhs.gov.

COUNTER-IMPROVISED EXPLOSIVE DEVICE (IED) PROGRAMS AND RESOURCES

Counter-IED & Risk Mitigation Courses and Resources. To reduce risk to the Nation's critical infrastructure, NPPD's Office for Bombing Prevention (OBP) develops and delivers a diverse curriculum of training to build nationwide counter-IED core capabilities and enhance awareness of terrorist threats. Coordinated through State Homeland Security Officials and training offices, 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. Available courses are listed below. For more information, visit http://www.dhs.gov/bombing-prevention-training. To request training, contact your local Protective Security Advisor (PSA) or contact OBP@hq.dhs.gov.

- Bomb-making Materials Awareness Program (BMAP)
- Bomb Threat Management

Workshop
- IED Counterterrorism Workshop
- IED Search Procedures Workshop
- Protective Measures Course
- Surveillance Detection Course for Law
- Enforcement and Security Professionals
- Vehicle Borne IED (VBIED) Detection Course

Counter-IED & Risk Mitigation Products. The following products are made available from OBP and can be found at http://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
- Incident Management Preparedness and Coordination Toolkit (IMPACT)
- Protective Measures Guidance
- VBIED Identification Guide: Parked Vehicles
- Vehicle Inspection Guide (VIG) & Video

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.

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 24/7 online, collaborative information-sharing network for bomb technicians, first responders, military personnel, government officials, intelligence analysts, and select private sector security professionals 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 also regularly used to share critical information with our federal, state, local, tribal, territorial, and private sector security partners during periods of heightened alert or following IED related incidents. TRIPwire is available at no cost to registered subscribers at https://tripwire.dhs.gov, and features a public-access homepage with valuable preparedness information for the whole community. For additional information, contact OBP@hq.dhs.gov.

CYBERSECURITY

United States Computer Emergency Readiness Team (US-CERT) Portal is a web-based information sharing portal that enables members to exchange actionable cybersecurity information with other practitioners. The National Cybersecurity & Communications Integration Center's (NCCIC) operational branches, including US-CERT, share cyber threat indicators, alert, and warning information, and analytical findings through structured Portal 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 **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 www.gsa.gov/cdm.

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 Homeland Security Information Network (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 CSEP program at CSE@dhs.gov.

Cybersecurity Evaluation Program (CSEP) conducts voluntary cybersecurity assessments across all 16 critical infrastructure sectors (including the Emergency Services Sector) and within state governments and large urban areas. CSEP affords critical infrastructure and key resources sector participants a portfolio of assessment tools, techniques, and analytics, ranging from those that can be self-applied to those that require expert facilitation or mentoring outreach. The CSEP works closely with internal and external stakeholders to measure key performances in cybersecurity management. The Cyber Resiliency Review is being deployed across all 16 critical infrastructure sectors, state, local, tribal, and territorial governments. For more information, visit www.us-cert.gov/ccubedvp/self-service-crr or contact CSE@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 http://ics-cert.us-cert.gov/Information-Products.

Emergency Services Sector-Cyber Risk Assessment (ESS-CRA). The 2012 ESS-CRA is the first ESS-wide cyber risk assessment that analyzes strategic cyber risks to ESS infrastructure. The ESS-CRA process provides a national-level risk profile that ESS partners can use to prioritize how they spend resources and where to focus training, education, equipment investments, grant requests, and further study. The risk assessment consisted of seven evaluation sessions to solicit input from ESS subject-matter experts. Each scenario evaluated threats, vulnerabilities, and consequences to ESS cyber infrastructure. Stakeholders

chose scenarios based on what would have the widest impact - the scenarios likely to affect the most disciplines at a time. The final ESS-CRA report includes a risk profile showing how the scenarios would affect each discipline, and the operational impact. Cyber risks to each discipline are ranked from high to low in terms of likelihood and consequence. The assessment approach is not intended to be guidance for individual entity's risk management activities. Instead, by increasing the awareness of risks across the public and private sector domains, the ESS-CRA serves as a foundation for ongoing national-level collaboration to enhance the security and resilience of the ESS disciplines. If you have any questions about the ESS Cyber Risk Assessment, please 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 government groups) 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 block certain types of malicious traffic from entering customer networks. Groups interested in receiving ECS services should

visit http://www.dhs.gov/enhanced-cybersecurity-services for more information.

Federal Virtual Training Environment (FedVTE) is an online training center featuring a wide range of cybersecurity courses – to state, local, tribal, and territorial government employees across the country. FedVTE provides government-wide, on-demand access to cybersecurity training to help the workforce maintain expertise and foster operational readiness at no cost to users. Courses range from beginner to advanced levels and is accessible from any internet-enabled computer. For more information, visit the National Initiative for Cybersecurity Careers and Studies portal at: 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 http://www.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 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 http://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 http://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, federal, state, local, tribal, and territorial governments with a role in protecting the IT Sector. For more information, visit 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 24x7 MS-ISAC Security Operations Center, or visit http://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.

National Cybersecurity Assessment and Technical Services Team (NCATS). The National Cybersecurity Assessment and Technical Services (NCATS) team supports the NCCIC 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, please contact NCATS_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 NCCIC, 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. National Cyber Security Awareness Month, the capstone event of the 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 and increasing the resiliency of the nation in the event of a cyber incident. To learn more about NCSAM and

find out how to get involved, please contact the Campaign at stopthinkconnect@dhs.gov or visit 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 on the State, Local, Tribal, and Territorial Cybersecurity Engagement Program, 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 areas of responsibility. Under the guidance of a multi-agency review board, the DHS, the 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, please contact SLTTCyber@hq.dhs.gov.

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 President Obama'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 Internatioanl 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 www.dhs.gov/stopthinkconnect. or contact the Campaign at stopthinkconnect@dhs.gov.

United States Computer Emergency Readiness Team (US-CERT) responds to major incidents, analyzes threats and exchanges critical cybersecurity information with trusted

partners around the world. US-CERT is working more closely than ever with partners to develop a comprehensive picture of malicious activity and mitigation options.

In its role as the federal information security incident center, US-CERT accepts incident notifications 24x7x365. 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 www.kb.cert.org/vuls, http://web.nvd.nist.gov/view/vuln/search, contact info@us-cert.gov or call 888-282-0870.

The **Critical Infrastrucure 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 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 and protective security services, leveraging the intelligence and information resources of our network of federal, state, local, tribal, territorial and private sector partners. FPS provides security planning; stakeholder engagement; law enforcement and information sharing services; and incident response.

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, 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.

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. 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 Crisis Response Teams 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, Uniformed Operations Division at 703-235-6080 or Robert.Scott4@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 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 http://training.fema.gov/EMIWeb/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/EMIWeb/IS/courseOverview.aspx?code=IS-921.a

- *Active Shooter: What You Can Do (IS-907)*, which uses interactive scenarios and videos to illustrate how individuals who become involved in an active shooter situation should react. For more information, visit http://training.fema.gov/EMIWeb/IS/IS907.asp.

- *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 http://training.fema.gov/EMIWeb/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 http://training.fema.gov/EMIWeb/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 http://training.fema.gov/EMIWeb/IS/IS912.asp.

- *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)

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, please contact the NICC.

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.

National Infrastructure Coordinating Center (NICC). The 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.

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 provides risk analysis tradecraft training to Fusion Centers. For access to risk analysis training call 202-282-8866 or e-mail FusionCenterSupport@hq.dhs.gov. For questions or requests, contact OCIA@hq.dhs.gov.

Protected Critical Infrastructure Information (PCII) Program

Are you finding it difficult to obtain the vital critical infrastructure information (CII) needed to support your critical infrastructure initiatives? Are private industry partners reluctant to share their data with you, 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 their 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 us at 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 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 coordinate improvised explosive device (IED) awareness and IED risk mitigation training. For more information or to contact your local PSA, contact PSCDOperations@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, 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 the Auxiliary Communicator and volunteer 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 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 www.dhs.gov/necp 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 are offered through the OEC TA Catalog that can be viewed on the PSTools site at: www.publicsafetytools.info. These offerings are at no-cost and can be requested through Statewide Interoperability Coordinators. 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 event, 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 evaluate their organization's connectivity and suggest 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 your 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: www.dhs.gov/gets; www.dhs.gov/wps; www.dhs.gov/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 them meet their communications and interoperability needs. For more information, visit www.safecomprogram.gov, 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 www.safecomprogram.gov/grant/Default.aspx 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 www.dhs.gov/statewide-communication-interoperability-plans.

DHS Privacy Office (PRIV)

PRIV protects all individuals regardless of citizenship 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 www.dhs.gov/privacy to share its experience and work products with DHS's partners and the public.

PRIV is always available to support our state and local partners. Please feel free to contact us 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 www.dhs.gov/privacy-investigations-compliance-reviews.

Privacy Compliance program, guidance, and templates. PRIV operates a robust privacy compliance program, using the

PIA 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 www.dhs.gov/privacy-compliance.

Policy Establishing the Fair Information Practice Principles as a matter of Department procedure. DHS believes in 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 PIAs of existing programs. DHS memorialized these principles as department policy. For more information, visit www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

Policy Establishing the Privacy Impact Assessment as a standardized government privacy compliance process. PRIV uses a structured approach to build privacy protections into specific programs: The PIA. DHS formally established the PIA requirement as a matter of policy. For more information, visit 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 www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf.

Privacy Outreach & Education. PRIV shares its experience directly with the public and its partners in the public, private, and academic sectors. For more information, visit 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 www.dhs.gov/sites/default/files/publications/privacy/Guidance/handbookforsafeguardingsensitivePII_march_2012_webversion.pdf.

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 them achieve their missions. S&T customers include the operating components of the Department, and state, local, tribal, and territorial emergency responders and officials.

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 www.dhs.gov/science-and-technology/centers-excellence.

The **First Responders Group** is S&T's component that works directly with first responder organizations to identify and prioritize gaps in capabilities,

establish operational requirements and standards, and develop and commercialize solutions. Projects in the First Responders Group's four strategic priority areas – communications, data sharing, first responder safety and effectiveness, 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, FRG has worked to ensure that technologies developed in coordination with S&T are available to first responder communities nationwide; S&T's technologies are included in the Federal Emergency Management Agency's Authorized Equipment List that public safety agencies are authorized to purchase from with their federal grant dollars. For more information, visit www.dhs.gov/science-and-technology/first-responders.

FirstResponder.gov is a website that enables federal, state, local, tribal, and territorial first responders to easily access and leverage federal resources on products, standards, testing and evaluation, and best practices to develop or deploy technologies to enhance homeland security. The website provides original content through blogs and articles, which highlight federal programs, initiatives, webinars, and research. "Technology Profiles" display DHS-funded

research and technologies by state. FirstResponder.gov also categorizes information by discipline: medical, explosives, fire, hazardous materials, law enforcement, and search and rescue. The website also provides a user feedback mechanism via email at: first.responder@dhs.gov. Visit www.firstresponder.gov.

First Responder Communities of Practice is an online network, sponsored by DHS Science and Technology First Responders Group, for vetted active and retired first responders, emergency response professionals; federal, state, local, tribal, and territorial Homeland Security and government officials, academic, non-profit, and volunteers sponsored by the DHS S&T's First Responder Technologies program. Registered members of this professional network 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 7,000 active members and nearly 200 active communities based on diverse interests and disciplines. For more information, visit www.firstresponder.gov or https://communities.firstrespond er.gov.

The **First Responder Resource Group (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. To learn more about the FRRG, contact SandTFRG@dhs.gov.

International Consortium for First Responder Research and Development is being established by FRG to collaborate with international partners to consolidate common first responder capability gaps; share knowledge and networks with industry, academia, developers and innovators; and support the aggregation of the global first responder market. In order to respond more effectively, safely, and efficiently to everyday and catastrophic emergencies, first responders around the globe need technologically advanced tools and equipment. However, there is no centralized mechanism for them to identify and discuss shared needs and requirements. In addition, they tend to purchase tools and equipment in small quantities, which provides little incentive for industry to commercialize

innovative technologies. The lack of consolidated requirements for first responders, along with the limited purchasing, results in an inadequate amount of new technology being available. This leads to an insufficient amount of research & development (R&D) being conducted in the first responder market. The goal of the International Consortium for First Responder R&D is to work collaboratively with international partners to improve first responder capabilities. To learn more about the International Consortium for First Responder R&D contact SandTFRG@dhs.gov.

The **National Urban Security Technology Laboratory (NUSTL)** is tasked with the mission to test, evaluate, and analyze Homeland Security capabilities while serving as a technical authority to first responder, state, and local entities in protecting our cities. In executing its mission, the Laboratory serves as a federal technical authority promoting the successful development and integration of homeland security technologies into operational end-user environments by objectively:

- Conducting test programs, pilots, demonstrations, and other forms of evaluations of homeland security technologies, both in the field and in the laboratory.
- Leveraging knowledge of end-user operations for

more effective development of technologies, training and exercises, ConOps, and procedures.

- Enabling first responders to meet their mission requirements by supporting them in the development of operational requirements and advising them on potential solutions to meet these needs.
- Supporting development and use of homeland security equipment and operational standards.

For more information, visit www.dhs.gov/science-and-technology/national-urban-security-technology-laboratory.

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, developB and promulgate standards through InterAgency Board's (IAB) 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 bomb squad robots, personal protective equipment, urban search and rescue robots, communications equipment, chemical and biological detectors among others that directly address needs expressed by the law enforcement community. For more information, contact Standards@hq.dhs.gov.

Project 25 Compliance Assessment Program (P25 CAP) was established, in coordination with NIST, 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 standards are focused on developing radios and other components 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. A DHS-approved laboratory is authorized to produce summary and detail test reports for P25 equipment. For more information, visit www.llis.dhs.gov/knowledgebase/certifications-declarations.

The **Responder Technology Alliance (RTA)** was established by FRG to reframe the discussion among first responders, 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 focus areas are: (1) Body-Worn Electronic Systems; (2) Integrated Voice and Data Communications; (3) Multiple Hazard Personal Protective Clothing and Equipment (PPE); and (4) Advance Sensors and Information Technologies. 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 about RTA contact SandTFRG@dhs.gov.

System Assessment and Validation for Emergency Responders (SAVER) Program assists emergency responders making procurement decisions by providing subjective assessments of commercial responder equipment and systems. SAVER provides those assessment results along with other relevant responder equipment information in an operationally useful form. SAVER focuses primarily on answering two questions: "What equipment is available?" and "How does it perform?" The Knowledge Products produced by the SAVER Program are available to the responder community through www.firstresponder.gov/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, federal partners, and 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 VQiPS@hq.dhs.gov

Virtual Training provides a virtual environment that every jurisdiction within the country will be able to access, train within, and modify to meet their individual needs. S&T is leveraging investments and technological advances made by the military, specifically the U.S. Army's prototype virtual environment called Enhanced Dynamic Geo-Social Environment (EDGE) Virtual Training. S&T is using EDGE to develop a series of realistic, first responder-identified scenarios. The scenarios will have varying levels of difficulty and will require users to successfully employ tactics, techniques, and procedures to respond. The tool also has a strategic component requiring responders to establish Unified Command to manage complex cross discipline events. S&T worked with first responders to identify critical incidents and chose an active shooter for the first scenario and with the U.S. Army to create a 3-D environment for the scenario, as well as accurate avatars, equipment, and simulations of individuals and crowds. Following initial development, S&T conducted a pilot to demonstrate this scenario with

emergency response agencies in Sacramento, California, and is currently upgrading EDGE with feedback collected from the Sacramento exercise. Eventually, S&T plans to incorporate this scenario, as well as others, into a customizable, multi-player online game that is interoperable with multiple user interfaces (e.g., joy stick, keyboard, gaming console). To learn more about simulation tools for first responders, contact SandTFRG@dhs.gov.

United States Secret Service (Secret Service)

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.

Computer Emergency Response Team (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 Computer Emergency Response (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 does distribute 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 digital equipment and information obtained through 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 your local Secret Service Field Office at http://www.secretservice.gov/contact/field-offices/ or contact your local ECTF at http://www.secretservice.gov/investigation/#field.

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: the eLibrary, a unique collection of resource databases which allows authorized users from throughout the law enforcement community to obtain information on a range of sensitive topics including counterfeit corporate checks, credit card issuing bank information, and recovered skimming devices; and the 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 specialists conduct forensic examinations of computers, mobile devices,

and other electronic media. These agents possess the required expertise to collect and process digital evidence to support computer related investigations in the field. They also provide expertise in the investigations of network intrusions and database thefts. The program provides a venue that establishes and maintains relationships with the private sector in order to sustain and continually improve its knowledge of emerging trends in the cyber industry. ECSAP agents conduct forensic examinations for other federal, state, or local law enforcement upon request. For more information, please contact your local Secret Service Field Office at http://www.secretservice.gov/investigation/#field or contact your local ECTF at http://www.secretservice.gov/investigation/#field.

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 to *"prevent, detect and investigate various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems."* There are currently 39 Secret Service ECTFs, to include London, England and Rome, Italy. Membership in

the Secret Service ECTFs include approximately 350 academic partners; over 2,500 international, federal, state, and local law enforcement partners; and over 4,000 private sector partners. Through the ECTFs, local and state law enforcement officers may request investigative assistance from the Secret Service's Mobile Wireless Investigations teams. There are currently 22 MWI teams throughout the United States. For more information, visit http://www.secretservice.gov/investigation/#field. Also see ICE section above.

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 your local Secret Service Field Office at http://www.secretservice.gov/contact/field-offices/.

Financial Crimes Task Forces (FCTF). The Secret Service through years of collaboration on investigative endeavors established unique partnerships with state, local, and other Federal law enforcement agencies. Leveraging those partnerships with the agencies long-standing cooperation with the private sector, the Secret Service established a national network of Financial Crimes Task Forces (FCTFs). The FCTFs combine the resources of the private sector and other law enforcement agencies in an organized effort to combat threats to our financial payment systems and critical infrastructures. The multi-agency components are well suited to conduct complex, in-depth, multi-jurisdictional investigations. Through their membership in a FCTF, local and state law enforcement entities may access investigative resources to include FinCEN, INTERPOL, and IOC-2 databases. For more information, please contact your 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 your 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 your local Secret Service Field Office at

National Center for Missing and Exploited Children. The Secret Service supports the National Center for Missing and Exploited Children 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/image enhancement and speaker recognition services. Specialized polygraph and crime scene services are evaluated upon request. For more information, visit http://www.missingkids.com/home and http://www.secretservice.gov/investigation/#forensic.

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, 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, Immigration and Customs Enforcement, the Joint Terrorism Task Force, Customs and Border Protection, 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 the TSA Website 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 Center (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 their 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 online at https://www.tsa.gov/stakeholders/resources-and-reports-1 or write to TSA-Surface@tsa.dhs.gov.

DVD Training – *Protecting Pipeline Infrastructure: The Law Enforcement Role*. Identifying a gap in the existing training materials, TSA developed this DVD training program to enhance the understanding of pipeline systems and their security issues by law enforcement officials. This DVD provides a basic understanding of how pipeline systems function, the principal products they transport, as well as a description of the threats to, and vulnerabilities of, pipelines. Law enforcement officials will achieve a better understanding of the usual measures taken to protect pipelines, and actions they can take to assist in this effort during times of heightened security. For more information

and to order your training materials, visit www.tsa.gov/stakeholders/training-and-exercises.

First Observer Security™ 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 currently available for highway-related professions. A new generation of messages similarly created will focus on those working in mass transit, passenger and freight rail and pipeline modes. More than 96,000 civilian transportation workers have been trained to date and TSA's domain awareness programs have been directly credited with disrupting two terrorist events. Learn more by writing to FirstObserver@tsa.dhs.gov or online at https://www.tsa.gov/first-observer.

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, test emergency procedures, and sharpen skills in incident management. I-STEP builds partnerships by collaborating with modal partners, law enforcement personnel, first responders, medical professionals, government leaders, and industry representatives to address challenges in transportation security. For more information, contact the I-STEP Program Office at 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 http://exis.tsa.dhs.gov. For more information, contact EXIS@dhs.gov.

Joint Vulnerability Assessment (JVA) Training. The Security Assessments Section (SAS), under the Office of Law Enforcement/Federal Air Marshal Service, Security Services and Assessments Division conducts JVAs in partnership with the FBI for the purpose of assessing current and potential threats to commercial air transportation facilities within the United Sates. The assessment process is a direct result of the increasing threat to aviation, a threat which prompted Congress to pass Section 310 of the Federal Aviation Reauthorization Act of 1996, requiring the Federal Aviation Administration (FAA) and the FBI to conduct joint threat and vulnerability assessments of security at U.S. airports. In response to this mandate, during Fiscal Years (FY) 1999, 2000, and 2001, FAA and FBI prepared three-part assessments addressing the vulnerability, criminal activity, and terrorist threat at selected airports nationwide. In Fiscal Year 2002, TSA took on the responsibility of conducting assessments from the FAA pursuant to the Aviation and Transportation Security Act. SAS conducts JVAs in order to identify vulnerabilities and recommends options to mitigate those vulnerabilities. SAS conducts JVA training as needed and it can be made available to local law enforcement and security personnel upon request. For more information, contact OLEFAMSSAS@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, visit www.tsa.gov/about-tsa/law-enforcement-officer-leo-reimbursement.

Man-Portable Air Defense Systems (MANPADS) Awareness Training. MANPADS are portable surface to air guided missile systems designed to be carried by an individual. The SAS, under the Office of Law Enforcement/Federal Air Marshal Service, Security Services and Assessments Division, 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. 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@dhs.gov.

Canine Training Center (CTC). The Office of Training and Workforce Engagement CTC supports the TSA mission by providing highly trained Explosives Detection Canine teams for deployment throughout the Nation's transportation systems. The canine teams provide explosive detection capabilities, visible deterrence, and a timely and mobile response to security incidents. These highly trained canine teams are trained to work within the major transportation environments, i.e., aviation, maritime, mass transit surface, and rail, to detect various explosives odors. Detection capabilities include, but are not limited to, the following: aircraft, trains, ferries, cruise ships, vehicles, passenger terminals, cargo, baggage, as well as people and items either concealed on their person or in their possession. The capabilities provided by these canine teams offer a very proficient layer of security in our Nation's transportation systems in support of the TSA mission.

Sensitive Security Information (SSI) Program. Sensitive Security Information

(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@dhs.gov.

The **TSA Call 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 for alleged misconduct and an explanation of the issue, including date(s) and time(s). They are also 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 may also 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 Workforce Engagement, Law Enforcement and Industry Training 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 material may be obtained by emailing the TSA Office of Training and Workforce Engagement, Law Enforcement and Industry Training Division, at LEOFA@dhs.gov
To request 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;
➢ Send the request from a governmental email address; and
➢ Include the following information in the body of the email: (1) Your name and contact information; (2) Your department's name and address; and (3)

Your supervisor's name and contact information.

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) 359-5367 between the core business hours of 9:00 am to 5:00 pm EST.

Visible Intermodal Prevention and Response (VIPR) Program. Focusing on deterrence and detection of terrorist activities, TSA conducts VIPR operations that promote confidence in and protect all modes of transportation through targeted deployment of integrated TSA assets, coming from TSA's Offices of Law Enforcement and Security Operations.

The VIPR Program has a nationwide footprint. Applying a risk-based planning process, TSA conducts VIPR operations with state and local personnel on a random, unpredictable basis. VIPR operations are conducted in all modes of aviation and surface

transportation. Teams may also be deployed to provide additional law enforcement or security presence at transportation venues during specific alert periods or in support of special events.

The exact makeup of a VIPR operation team is determined jointly with local authorities. An operation can include Federal Air Marshals, Transportation Security Officers, Behavior Detection Officers, Transportation Security Inspectors, and Transportation Security Specialists – Explosives, TSA personnel can use explosives operational support, security and explosive screening technology, and radiological/nuclear detection equipment.

For more information on TSA's VIPR resources, visit the TSA website or contact your OLE/FAMS Supervisory Air Marshal in Charge (SAC) or Federal Security Director (FSD).

ACRONYMS

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

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

APPENDIX

3/1/16

W