DHS State and Local Law Enforcement Resource Catalog

Volume I

January 2013

Intentional Blank Page. Please Continue to Next Page.

Letter from Assistant Secretary Louis F. Quijas

January 18, 2013

Dear Law Enforcement Partners:

Homeland security begins with hometown security, and as part of our commitment to hometown security, 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*, I am 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 my office 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. I hope this catalog is another one of those tools that will assist in your efforts to keep our communities safe, secure, and resilient.

Sincerely,

Louis F. Quijas

Louis F. Quijas
Assistant Secretary
Office for State and Local Law Enforcement
Department of Homeland Security

Office for State and Local Law Enforcement

MISSION

The mission of the Office for State and Local Law Enforcement (OSLLE) is to formulate and coordinate national-level policy relating to law enforcement's role in preventing acts of terrorism, and to serve as the DHS's primary liaison with state, local, tribal, and territorial law enforcement personnel and agencies.

Office for State and Local Law Enforcement	
Component Integration Branch The Component Integration Branch ensures that offices and Components within DHS have a consistent and coordinated message to state and local law enforcement. Contact: 202-282-9545	**Mission Support Branch** The Mission Support Branch addresses the activities and programs within the Department that benefit from direct collaboration and support with state and local law enforcement. Contact: 202-612-1729
Law Enforcement Policy Branch The Law Enforcement Policy Branch ensures that the issues, concerns, and requirements of state and local law enforcement are taken into consideration during policy development and strategy formation. Contact: 202-612-1189	**Law Enforcement Grants & Training Branch** The Law Enforcement Grants and Training Branch identifies and disseminates training opportunities available to state and local law enforcement, as well as works with the Federal Emergency Management Agency (FEMA) to ensure that accurate, timely, and actionable information on law enforcement-related grants is made available to state and local law enforcement. Contact: 202-612-1164

OSLLE Contact Information:

Phone: 202-282-9545
Fax: 202-282-8306
Email: OSLLE@hq.dhs.gov
Website:
http://www.dhs.gov/office-state-and-local-law-enforcement

Table of Contents

U.S. Citizenship and Immigration Services Ombudsman (CISOMB)

The Ombudsman's Office (CISOMB) is available to help law enforcement with issues or concerns that they have regarding their interactions with USCIS. CISOMB is an independent, impartial, and confidential office within DHS that helps individuals and employers resolve problems with USCIS applications and petitions and also make 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 problems in the immigration benefits process and preparing recommendations for submission to USCIS for process changes. Recommendations for process changes should not only identify the problem experienced, but should also contain a proposed solution that will not only benefit an individual case, but others who may be experiencing the same problem as well. Send comments, examples, and suggestions to cisombudsman@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 a request to the Ombudsman using DHS Form 7001 (Case Assistance Form). To submit a request for assistance on behalf of somebody other than yourself, you should ensure that the person the case problem is about (the applicant for a USCIS immigration benefit, or the petitioner who seeks to obtain an immigration benefit for a third party) consents to your inquiry (see Submitting a Request for Case Assistance using DHS Form 7001). For more information, see http://www.dhs.gov/files/programs/editorial_0497.shtm.

U Visa Law Enforcement Certification Resource Guide. The U visa is an immigration benefit that can be sought by victims of certain crimes who are currently assisting or have previously assisted law enforcement in the investigation or prosecution of a crime, or who are likely to be helpful in the investigation or prosecution of criminal activity. This Guide provides law enforcement officials information about U visa requirements, the law enforcement certification process, and answers to frequently asked questions from law enforcement agencies to support investigations and prosecutions involving qualified immigrant victims of crime.
The U Visa Resource Guide is available as a print and electronic resource. Included in the guide is a selection of best practices and a FAQ section that draws upon questions received by state and local law enforcement. For more information see http://www.dhs.gov/xlibrary/assets/dhs_u_visa_certification_guide.pdf.

U.S. Citizenship and Immigration Services (USCIS)

U.S. Citizenship and Immigration Services (USCIS) assists individuals and employers in resolving immigration benefits problems, propose changes in administrative practices to improve customer service, and directly provide Congress and the Department of Homeland Security substantive analysis on the quality of immigration services.

USCIS Citizenship Resource Center is as a web-based portal that centralizes citizenship resources for immigrants, educators and organizations. This free, easy-to-use website helps users understand the naturalization process and gain the necessary skills to be successful during the naturalization interview and test. For more information, see http://www.uscis.gov/citizenship.

Civics and Citizenship Toolkit. A Collection of Educational Resources for Immigrants contains a variety of educational materials designed to help permanent residents learn more about the U.S. and prepare for the naturalization process. For more information, visit http://www.citizenshiptoolkit.gov

E-Verify is an Internet-based service through which an employer, using information reported on an employee's Form I-9, confirms an employee's eligibility of their newly hired employees to work in the U.S. There is no charge to enroll in the E-Verify program. Enrollment in the E-Verify program is voluntary for most employers, but mandatory for some, such as employers with federal contracts or subcontracts that contain the Federal Acquisition Regulation (FAR) E-Verify clause and employers in certain states that have legislation that mandates the use of E-Verify for some or all employers.

Available resources for employers and workers include searchable web pages, demonstration videos, guides on employee rights and employer responsibilities, fact sheets, free live webinars, an overview presentation, e-newsletter (E-Verify Connection) brochures, and posters. USCIS has an online multi-media employee rights toolkit to assist stakeholders and workers to understand employee rights in the employment eligibility verification process. E-Verify also has speakers available to give live presentations at conferences and meetings across the country. For more information on E-Verify visit http://www.dhs.gov/everify, email E-Verify@dhs.gov or the employers hotline at 888-464-4218/877-875-6028 (TTY) or the worker hotline at 888-897-7781 (TTY).

Expanding English as a Second Language (ESL), Civics, and Citizenship Education in Your Community: A Start-Up Guide provides an overview and recommendations to help organizations design and offer ESL and civics/citizenship classes for immigrants. For more information, see http://www.uscis.gov/USCIS/Office%20of%20Citizenship/Citizenship%20Resource%20Center%20Site/Publications/PDFs/M-677.pdf.

Form I-9, Employment Eligibility Verification is a form that U.S. employers must complete for each new employee hired after November 6, 1986. Completion of Form I-9 establishes that the employer has examined documentation from each newly hired employee to verify a new hire's identity and authorization to work in the U.S. Available resources (English and Spanish) include the I-9 Central website (a collection of helpful information for workers and employers covering how to properly complete the form, employee rights, avoiding errors and discriminatory practices); free webinars; the Handbook for Employers; Instructions for Completing Form I-9 (M-274); and the USCIS fact sheet: How Do I Complete Form I-9. For more information on Form I-9, visit I-9 Central (www.uscis.gov/I-9Central or www.uscis.gov/I-9Central/espanol) or http://www.uscis.gov or call 888-464-4218/877-875-6028 (TTY) or the worker hotline at 888-897-7781/877-875-6028 (TTY).

Guide to Naturalization contains information about the naturalization process, laws and regulations.
See http://www.uscis.gov/files/article/M-476.pdf.

USCIS Information for Employers and Employees is a website regarding the authorization verification process and the immigration petition process. Please visit www.uscis.gov and click on 'Information for Employers and Employees' under 'Working in the US' or click here. For more information contact Public.Engagement@dhs.gov.

The Law Enforcement Support Operation (LESO) Unit.
U.S. Citizenship and Immigration Services' (USCIS) 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" regarding criminal activity, who are willing to share their information with a U.S. agency or court and whose presence in the United States is necessary for the successful prosecution of the 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 ("cover") immigration documents are genuine immigration documents issued to individuals who do not possess the associated immigration status. These documents are issued in furtherance of covert operations, by creating 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, a concurrence memorandum is transmitted to USCIS for action in producing the requested document.

USCIS Office of Public Engagement (OPE) seeks to focus on open, candid, and constructive collaboration with community stakeholders at all levels. OPE coordinates and directs USCIS-wide dialogue with external stakeholders to advance the Agency's vision of customer

inclusiveness by actively engaging stakeholders to ensure information flow and to institutionalize a mechanism whereby their input will be considered in the process of policy formulation, priority calibration, and assessment of organizational performance. The goal of the office is to provide information and invite feedback to inform our work. See the Outreach tab at http://www.uscis.gov. For more information contact Public.Engagement@dhs.gov.

USCIS Resources offers a variety of resources including customer guides, videos, citizenship toolkits, an immigration law glossary, reports and studies, civics and citizenship education resources, and a historical library. See the "Resources" section at http://www.uscis.gov. For more information contact Public.Engagement@dhs.gov.

Self Check is a free online service of E-Verify that allows U.S. workers to confirm their own employment eligibility. It is the first online E-Verify service offered directly to workers. Available in English and Spanish, Self Check enables individuals to enter the same information into Self Check that employers enter into E-Verify. If a problem exists with their records related employment eligibility, Self Check explains how to resolve that issue. Job seekers are encouraged to use Self Check to make sure their records are in order. The Self Check site also has an information tool kit with materials that can be distributed to increase awareness of the service. For more information on Self Check, please visit www.uscis.gov/selfcheck or www.uscis.gov/selfcheck/espanol, email

T and U Visas for Victims of Human Trafficking and Other Serious Crimes. The T and U visa programs are available for victims of human trafficking and other serious crimes who are cooperating with law enforcement in the investigation or prosecution of the crime. Federal, State, and local law enforcement agencies may sign a law enforcement certification for the victim detailing the crime and the cooperation of the victim in the investigation or prosecution. The victim must then apply to USCIS for a T or U visa. The investigating or prosecuting law enforcement agency does not request a visa for the victim to USCIS. Once the victim applies for a T or U visa, USCIS reviews the application and all submitted evidence to determine eligibility.

More information on T and U visas can be found at www.uscis.gov/humantrafficking and http://www.dhs.gov/blue-campaign.

United States Coast Guard (USCG)

The United States Coast Guard (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 (ASB) and Landing Craft. The USCG cutter fleet ranges from a 425-foot Icebreaker to a 65-foot harbor tug, however, most commonly recognized and widely utilized are High and Medium Endurance Cutters (210-foot, 270-foot, 378-foot) and our smaller 87-foot and 110-foot patrol vessels.

There are a total of 211 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 turboprops and HU-25 Falcon jets) 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; CBRNE Detection and Identification; Disaster Response; Environmental Response; Deployable Incident Management; Advanced Planning; and multiple supporting capabilities.

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/Group Command Centers. There are 38 USCG Sector/Group Commands throughout the U.S. and U.S. territories:

Sector Anchorage Command Center 907-229-8203	**Sector Key West Command Center** 305-292-8727
Sector Juneau Command Center 907-463-2000	**Sector Miami Command Center** 305-535-4472/ 4473/8701
Sector Mobile Command Center 251-441-6215 / 6211	**Sector St. Petersburg Command Center** 727-824-7506
Sector Los Angeles-Long Beach Command Center 310-521-3801	**Sector Guam Command Center** 671-339-6100
Sector San Diego Command Center 619-278-7030	**Sector Honolulu Command Center** 808-842-2600
Sector San Francisco Command Center 415-399-3530	**Sector Ohio Valley Command Center** 502-779-5422
Sector Long Island Command Center 203-468-4401 / 4402/4403/4404	**Sector New Orleans Command Center** 504-846-6160
Sector Jacksonville Command Center 617-223-5757	**Sector Boston Command Center** 713-671-5133
Sector Detroit Command Center 313-568-9560 / 9559	**Sector Hampton Roads Command Center** 757-668-5555 / 757-638-6635
Sector Northern New England Command Center 207-767-0303	**Sector Seattle Command Center** 206-217-6002
Sector Baltimore Command Center 410-576-2525 / 2693	**Group/Air Station Port Angeles** 360-417-5840
Sector Sault Ste Marie Command Center 906-635-3233	**Sector Lake Michigan Command Center** 414-747-7182
Sector North Carolina Command Center 252-247-4572	**Sector Southeastern New England Command Center** 508-457-3211
	Sector Charleston Command Center 843-724-7616
Sector Upper Mississippi River Command Center 314-269-2332/2463	**Sector Lower Mississippi Command Center** 901-521-4824
Sector Buffalo Command Center 716-843-9525	**Sector Corpus Christi Command Center** 361-939-6393 / 6349
Sector New York Command Center 718-354-4353 / 4193	**Sector Delaware Bay Command Center** 215-271-4960
Group/Air Station Astoria 503-861-6211	**Sector San Juan Command Center** 787-289-2041
Sector North Bend 541-756-9210	**Sector Houston-Galveston** 713-678-9011 707-839-6117
Sector Portland Command Center 503-240-9311	
Sector Humboldt Bay Command Center	

Office for Civil Rights and Civil Liberties (CRCL)

The DHS Office for Civil Rights and Civil Liberties (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 ICE and other DHS 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.

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 statues.

Information for recipients on meeting their nondiscrimination requirements under Title VI is available on CRCL's website, http://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 (LEP), http://www.dhs.gov/guidance-published-help-department-supported-organizations-provide-meaningful-access-people-limited). For more information, please contact crcl@dhs.gov.

Civil Rights Training for State and Local Law Enforcement on the ICE 287(g) Program and Secure Communities. CRCL provides training on civil rights protections and the intersection of state and local enforcement of immigration law. Topics covered include communication with limited English proficient individuals, racial and ethnic profiling, consular notification requirements, and best practices for adhering to ICE detainers.

Common Muslim American Head Coverings and Common Sikh American Head Coverings Training Presentation and 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.
Duration of Presentation: N/A.
Available from: CRCL's website: http://www.dhs.gov/xabout/structure/gc_1282160124874.shtm.

Educational posters in customizable digital and hard copy form can be ordered from the DHS Office for Civil Rights and Civil Liberties by e-mailing crcltraining@dhs.gov.

Community Roundtables. CRCL leads, or plays a significant role, in regular roundtable meetings across the country in over fourteen U.S. cities. These roundtables bring exceptionally diverse demographic communities together with Federal, state, and local 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 please contact communityengagement@hq.dhs.gov

Countering Violent Extremism (CVE) training. In accordance with the White House's National Security Strategy and the DHS HSAC Recommendations on Countering Violent Extremism, CRCL created a training program designed to increase the cultural competency of law enforcement and encourage community-oriented policing partnerships between law enforcement and community groups. Topics of discussion include: an unclassified threat briefing; misconceptions and stereotypes of Islam and Muslims; a how-to guide for community interaction; effective policing without the use of racial or ethnic profiling; and the U.S. Government's approach to engagement and outreach.
Duration: Flexible based on needs. Generally, 2-4 hours of instruction.
For more information: E-mail CRCLtraining@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 countering violent extremism, cultural awareness, and counterterrorism training.
For more information: Please visit CRCL's website: http://www.dhs.gov/xabout/structure/gc_1282160124874.shtm.

CRCL Facebook Page. As one of the few DHS Headquarters offices that engages directly with the public, CRCL utilizes its Facebook page to increase and deepen its regular contact with community stakeholders, and also reach and inform a wider audience on the CRCL's work to incorporate civil rights and civil liberties protections into DHS programs and activities.

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, please visit www.dhs.gov/crcl.

CRCL Newsletter is distributed monthly to inform our stakeholders and the public about Office activities, including how to make complaints; ongoing and upcoming projects; opportunities to offer comments and feedback; etc. Newsletters are distributed via an email list to thousands of NGOs, community members, and government partners, and made available to community groups for redistribution. Please contact CRCLOutreach@dhs.gov for more information.

Equal Employment Opportunity (EEO) Reports. CRCL EEO & Diversity Division prepares and submits a variety of annual progress reports relating to the Department's EEO activities. For more information please visit www.dhs.gov/crcl.

E-Verify and Unfair Labor Practices Training is provided by CRCL on the worker rights and the responsibilities imposed upon the private sector when using E-Verify and verifying employment eligibility. Training includes best practices, examples of unlawful practices against workers, remedies for workers, and instructions for how to prepare a human resources department. The training assists employer understanding of how to use E-Verify in a responsible manner without violating prohibitions against discrimination. In collaboration with U.S. Citizenship and Immigration Services, CRCL has created two videos, *Understanding E-Verify: Employer Responsibilities and Worker Rights* and *Know Your Rights: Employee Rights and Responsibilities*, to ensure employers and employees are knowledgeable about their rights and responsibilities. To view the videos, please visit www.dhs.gov/E-Verify or www.youtube.com/ushomelandsecurity. For more information, contact CRCL at crcltraining@dhs.gov or 1-866-644-8360.

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.
Available from: CD-ROM can be ordered from CRCL by e-mailing crcltraining@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 the Department of Homeland Security. Complaints are accepted in languages other than English.
For more information: Please visit www.dhs.gov/crcl.

Human Rights and Vulnerable Populations. CRCL is the DHS single point of contact for international human rights treaty reporting and coordination. In coordinating treaty reporting for the Department, CRCL works across DHS and with other Federal agencies and departments. At DHS, CRCL also ensures that U.S. human rights obligations are considered in Department policies and programs. For more information please contact HumanRightsOfficer@hq.dhs.gov

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 United States 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, contact crcltraining@dhs.gov or visit http://www.dhs.gov/civil-rights-and-civil-liberties-institute.

Office for Civil Rights and Civil Liberties Quarterly and Annual Reports to Congress. Under 6 U.S.C. § 345 and 42 U.S.C. § 2000ee-1, CRCL is required to report annually to Congress about the activities of the Office. For more information, see http://www.dhs.gov/reports-office-civil-rights-and-civil-liberties.

Privacy, Civil Rights & Civil Liberties Fusion Center Training Program. The Implementing Recommendations of the 9/11 Commission Act requires that DHS support fusion centers in 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 State and Local Program Office and the DOJ Bureau of Justice Assistance to deliver this training program. The program has are four elements: a website Resource center found at www.it.ojp.gov/PrivacyLiberty, a training of Privacy/Civil Liberties Officers program, technical assistance 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 (8 hours) but can be customized to shorter sessions.
For more information: E-mail FusionCenterTraining@dhs.gov.

Quarterly NGO Civil Rights / Civil Liberties Committee Meeting. CRCL hosts regular meetings with representatives of over 20 civil society organizations primarily working on matters at the intersection of immigration and civil and human rights. Assisted by extensive grassroots networks, Committee members articulate the concerns of organizations and communities across the country on these issues. The CRCL Officer meets quarterly with the Committee to identify systemic and policy concerns relevant to CRCL. For more information please contact CRCLOutreach@dhs.gov.

Secure Communities and Briefing Material for State and Local Law Enforcement. CRCL and ICE have collaborated to create a series of downloadable awareness briefings for state and local law enforcement on the civil rights and civil liberties issues that may arise in the implementation of Secure Communities. These short roll call/muster video briefs are supplemented by separate materials packets for leadership and trainers. Topics include what Secure Communities is (and is *not*), responding to immigration detainers, consular notification requirements, unlawful retaliation by private actors, protecting victims and witnesses of crime, and avoiding racial and ethnic profiling. For more information, visit http://www.ice.gov/secure_communities/crcl.htm.

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 U.S. This video was developed by the Department of Justice Community Relations Service and reproduced by DHS.
Duration: 10 minutes.
Available from: CRCL's website: http://www.dhs.gov/xabout/structure/gc_1282160124874.shtm
This site also offers a transcript and limited resources and glossary.
Available from: DVD can be ordered from the CRCL by e-mailing crcltraining@dhs.gov.

Web Portal for Fusion Centers on Privacy, Civil Rights & Civil Liberties. 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. The web portal, launched on April 1, 2009, contains over 35 pages of new content and more than 400 links to key Federal resources. The portal was developed as a result of a partnership between CRCL and the DOJ.
Available at: http://www.it.ojp.gov/PrivacyLiberty.

U.S. Customs and Border Protection (CBP)

U.S. Customs and Border Protection is one of the DHS' largest and most complex components, with a priority mission of keeping terrorists and their weapons out of the U.S. 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 drug laws. For more information, see www.cbp.gov or contact 202-344-1700.

Carrier Liaison Program (CLP) 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 CLP, visit http://www.cbp.gov/xp/cgov/travel/inspections_carriers_facilities/clp/ or contact CLP@dhs.gov or 202-621-7817.

CBP Border Community Liaison Program. Border Community Liaisons (BCL) focus on outreach to community stakeholders and provide fact-based information regarding the CBP mission, functions, authorities, and responsibilities. BCLs 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 via the CBP.GOV website at https://help.cbp/app/home

CBP Laboratories and Scientific Services coordinates technical and scientific support to all CBP trade and border protection activities. For more information, visit http://www.cbp.gov/xp/cgov/newsroom/fact_sheets/lab_services.xml.

Electronic System for Travel Authorization (ESTA) is an automated system that determines the eligibility of visitors to travel to the U.S. under the Visa Waiver Program. The ESTA application collects the same information collected on Form I-94W. ESTA applications may be submitted at any time prior to travel, though it is recommended travelers apply when they begin preparing travel plans. Travelers participating in this program are required to pay a $14.00 travel fee with their ESTA application. For more information, see https://esta.cbp.dhs.gov/ or www.cbp.gov/ or contact at 877-227-5511 or 202-344-3710.

Intellectual Property Rights. CBP's IPR Help Desk provides information in 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 United States, 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, please visit: http://cbp.gov/xp/cgov/toolbox/contacts/ports/.

No te Engañes (Don't be Fooled) is the CBP outreach campaign to raise awareness among potential migrants. For more information, please visit http://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 visitors entering the United States. For a list of ports, please 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 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 (SLT). A component of the CBP Commissioner's Office, the State, Local, and Tribal Liaison (SLT) 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 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 36 countries to travel to and enter the United States for business or visitor purposes for up to 90 days without obtaining a visa. For more information about the Visa Waiver Program, please visit http://www.cbp.gov/xp/cgov/travel/id_visa/business_pleasure/vwp/.

Domestic Nuclear Detection Office (DNDO)

The Domestic Nuclear Detection Office (DNDO) is a jointly staffed office within the Department of Homeland Security. DNDO is the primary entity in the U.S. government for implementing domestic nuclear detection efforts for a managed and coordinated response to radiological and nuclear threats, as well as integration of federal nuclear forensics programs. Additionally, DNDO is charged with coordinating the development of the global nuclear detection and reporting architecture, with partners from Federal, state, local, and international governments and the private sector. For more information, see http://www.dhs.gov/about-domestic-nuclear-detection-office or contact DNDO.INFO@hq.dhs.gov.

Equipment Test Results. Federal, state, local, and tribal agencies intending to purchase radiological and nuclear (rad/nuc) detection equipment are strongly encouraged to consider only instruments that have been independently tested by accredited laboratories and have demonstrated conformity with the applicable 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 described below that are available to assist Federal, state, local and tribal entities in selecting the right rad/nuc 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 inform the rad/nuc detection procurement decisions of Federal, state, local, and tribal entities. Several of these test campaign results are available on the PRND COI and the Responder Knowledge Base (RKB) at http://www.rkb.us, while others may be requested by contacting DNDO at DNDO.INFO@hq.dhs.gov.

Examples of test reports include: Anole Test Campaign Report for handheld, backpack, and mobile systems (available on COI and RKB); Bobcat Test Campaign Report for commercial-off-the-shelf and prototype personal radiation detectors (PRDs); Crawdad and Dolphin Test Campaign Reports for boat-mounted detection systems (available upon request); Gryphon Test Campaign Report for aerial detection systems.

Exercises. DNDO provides assistance in developing, designing, and conducting exercises that are compliant with the Homeland Security Exercise and Evaluation Program (HSEEP) methodology. The exercises provide valuable hands-on experience for personnel performing radiation detection missions and assist decision makers in integrating the PRND mission into their daily operations. Additional information about PRND exercises is available by contacting DNDO at DNDO.SLA@hq.dhs.gov.

The GRaDER® Program
GRaDER® provides objective and reliable performance testing information to federal, state, and local stakeholders for radiological and nuclear detection equipment tested against consensus and technical capability standards to assist in making informed radiological and nuclear detection equipment procurements. Visit http://www.dhs.gov/GRaDER for further information or email GRaDER.questions@hq.dhs.gov.

Joint Analysis Center (JAC).
The Joint Analysis Center, housed in DNDO, provides awareness of the Global Nuclear Detection Architecture (GNDA) and provides technical support to Federal, state, and local authorities. Utilizing the Joint Analysis Center Collaborative Information System (JACCIS), the JAC facilitates radiological and nuclear (rad/nuc) 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 (NRC) 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 rad/nuc infrastructure that affects detection assets and response protocols.

JACCIS provides a process for Federal, state, tribal, territorial and local agencies to share radiological and nuclear detection information at the Unclassified/Official Use Only level. The JACCIS Dashboard provides a secure web interface to collaborate with mission partners and uses a geographic information system to show detection information, detectors, situational awareness reports, and other overlays in a geospatial viewer. Web service interfaces to other mission partner's systems and content routers provide linkages to detection assets around the country in real-time. JACCIS stores four types of National Information Exchange Model standardized message types that can be provided by these internet connected systems: rad/nuc alarms, an inventory of rad/nuc assets, rad/nuc sites, and rad/nuc situational awareness information. This same technology is employed to connect JACCIS to the TRIAGE system used by the Department of Energy to adjudicate alarms. This connection will allow a seamless transition of state, tribal, territorial, and local alarm adjudication in JACCIS to be elevated to TRIAGE for national-level adjudication assistance.

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: http://www.dhs.gov/xabout/structure/editorial_0766.shtm

Mobile Detection Deployment Program (MDDP). The ability to surge resources for use during special events, times of increased threat, or in response to information or events that indicate the need for enhanced detection capabilities is an important part of the GNDA. DNDO's Mobile Detection Deployment Program maintains trailer-based units outfitted with an extensive suite of radiation detection equipment and command and control capabilities. Modeled after DOE's Radiological Assistance Program (RAP) response system, these Mobile Detection Deployment Units (MDDUs) offer a national radiological and nuclear detection surge package that can be deployed as needed to assist stakeholders with augmenting their resident capabilities. The MDDUs are deployed regionally across the United States and maintained through an agreement with DOE RAP Teams. Each MDDU contains a number of mobile units, backpacks, high-resolution handheld devices, personal radiation detection devices, communications, and tracking equipment and is configured to outfit up to 40 personnel. The types of devices and numbers are carefully selected to optimize coverage and detection abilities while providing flexibility to the organizations supported. Each MDDU is accompanied by technical support staff to train personnel on the use of equipment and to help integrate these surge capabilities into existing operations. Deployment of a MDDU is authorized through the DNDO Operations Support Directorate (OSD) with the concurrence of DOE First Responder programs. Requests to use MDDU assets should be directed to DNDO at DNDO.SLA@hq.dhs.gov.

Open Access to 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/

PRND Program Management Handbook with Commercial Vehicle Inspection (CVI), Small Maritime Vessel Operations, and Special Events Modules and Technical Appendices. DNDO has developed a PRND Program Management Handbook with modules and technical appendices that address specific operational environments such as CVI, small maritime vessel operations, and special events. This handbook provides guidance for the administration of a domestic PRND program and is intended to assist program development and implementation at both the senior policy making and operational levels. The PRND PM Handbook and supporting resources can be obtained on the PRND Community of Interest (COI) web portal (see below) or by contacting DNDO at DNDO.SLA@hq.dhs.gov.

Preventive Rad/Nuc Detection (PRND) Community of Interest (COI) DNDO's PRND COI is located on the Homeland Security Information Network

(HSIN) and provides a repository for DNDO and other nuclear detection related information that can be accessed by external users and a forum where nuclear detection community stakeholders can collaborate and share best practices and lessons learned. State, local, and tribal 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 the Federal, state, local, and tribal levels are encouraged to join the site. To join the PRND COI, submit a request by email to DNDO with a message subject line of: "DNDO PRND COI HSIN Access Request" to the address: PRND_COI@hq.dhs.gov.

Radiological /Nuclear Detection and Adjudication Capability Development Framework (CDF). The CDF planning guidance assists state, local, and tribal jurisdictions with identifying and developing recommended levels of radiological and nuclear (rad/nuc) detection capability based on risk factors and the likelihood of encountering illicit rad/nuc material. The CDF is based on lessons learned provided by Federal, state, and local subject matter experts. It is intended to provide strategic guidance based on best practices, but not to establish specific requirements. The CDF is a DNDO product modeled on the FEMA Target Capability List (TCL) version 3.0, and can be leveraged to support investment justifications. A CDF Calculator is also available to assist jurisdictions with identifying recommended levels of rad/nuc detection capability quickly and easily. The CDF and supporting resources are available on the PRND Community of Interest (COI) web portal (see below) or by contacting DNDO at DNDO.SLA@hq.dhs.gov.

Securing the Cities (STC) Program. The Securing the Cities Program seeks to 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. The program assists Urban Areas selected through a competitive application process 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 Global Nuclear Detection Architecture (GNDA) and encourage participants to sustain the base nuclear detection program over time. There are three phases to the program; Phase I – STC assists state and locals to develop 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. 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. Phase III – STC 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 program support. For more information visit: http://www.dhs.gov/keywords/securing-cities or email DNDO.INFO@hq.dhs.gov.

Training. DNDO training provides quality products and support to develop, enhance, and expand radiological and nuclear (rad/nuc) detection capabilities in support of the GNDA. Together with Federal partners, the DNDO training program provides technical review, evaluation, and continual developmental improvement of the rad/nuc detection training curriculum to increase the operational detection capabilities of Federal, state, local and tribal agencies to detect and interdict rad/nuc materials and/or devices. The program seeks to develop and exercise protocols and training standards for effective use of radiation detection equipment and the associated alarm reporting and resolution processes and develop training curricula in support of emerging detection technologies and operational profiles. DNDO and its partners have completed rad/ncu detection training for over 23,000 law enforcement, first responder personnel and public officials through FY12.

Nuclear 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) training organization. CTOS Web page: http://www.ctosnnsa.org/. Courses are also available through the FEMA Federal

Sponsored Course catalog. FEMA FSCC Web page: https://www.firstrespondertraining.gov/webforms/pdfs/fed_catalog.pdf. DNDO can be contacted to discuss PRND training program questions, course needs, or special requests by emailing DNDOTRAINING@hq.dhs.gov.

Federal Emergency Management Agency (FEMA)

Federal Emergency Management Agency'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.

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, as supported by the *CPG 601: Design and Management of Emergency Operations Centers (future release)*. CPG 502 provides guidance on the broad capability requirements of an EOC.

FEMA Industry Liaison Program is a point-of-entry for vendors seeking information on how to do business with FEMA during disasters and non-disaster periods of activity. The program coordinates vendor presentation meetings between vendors and FEMA program offices, establishes strategic relationships with vendor-supporting industry partners and stakeholders, coordinates Industry Days, conducts market research, responds to informal Congressional requests, and performs vendor analysis reporting. Vendors interested in doing business with FEMA should take the following steps: Register in the Central Contractor Registration (CCR) at www.ccr.gov, contact the FEMA Industry Liaison Program at http://www.fema.gov/privatesector/industry/index.shtm, or call the Industry Liaison Support Center at 202-646-1895.

First Responder Training Web Site. National Training and Education Division (NTED) serves the nation's first responder community by offering more than 100 courses that help build the skills responders need to effectively function in mass consequence events. Course subjects range from Weapons of Mass Destruction (WMD) terrorism, cybersecurity, and agro-terrorism to citizen preparedness. The NTED Course Catalog provides valuable information about NTED's training courses and training providers, including course prerequisites and how to schedule and attend courses. The First Responder Training Web Site can be found at www.firstrespondertraining.gov.

Full-Spectrum Risk Database is a DHS/ FEMA website that provides a clearinghouse for baseline risk information and risk methodology templates and tools. FEMA grants access to users. The Full-Spectrum Risk Database can be found at https://riskknowledge.fema.gov.

Preparedness (Non-Disaster) Grants. FEMA provides state and local governments with preparedness program funding in the form of Non-Disaster Grants to enhance the capacity of state and local emergency responders to prevent, respond to, and recover from a weapons of mass destruction terrorism incident involving chemical, biological, radiological, nuclear, and explosive devices and cyber-attacks. For more information on how to find and apply for grants visit http://www.dhs.gov/how-do-i/find-and-apply-grants.
Ready to apply for a grant? Visit www.Grants.gov.

Responder Knowledge Base (RKB) serves as a resource to the state, local, and tribal homeland security responder community by providing information on commercial equipment and technology to assist them with purchasing and equipment decisions. The services include online, integrated sources of equipment-related information such as available FEMA grants, the FEMA Authorized Equipment List (AEL), equipment specifications, related certifications and applicable standards, test reports, the InterAgency Board (IAB) Standardized Equipment List (SEL), and other information. For more information visit: http://www.rkb.us.

Federal Law Enforcement Training Center (FLETC)

Contact Information:
Federal Law Enforcement Training Centers
Address: 1131 Chapel Crossing Road, Bldg. 2200, Glynco, GA 31524
E-mail: stateandlocaltraining@dhs.gov or
Phone: 800-743-5382 or 912-267-2345
Hours of Operation: 8 a.m. – 5 p.m. EST (Mon-Fri)

The Federal Law Enforcement Training Centers (FLETC) offers advanced and specialized law enforcement training in a variety of topics to state, local, rural, tribal, and territorial law enforcement officers and directly to host agencies throughout the United States and Indian country. Please visit www.fletc.gov/osl or www.fletc.gov/rpi for further information. In addition, tuition, room and board for state, local, rural, tribal, and territorial officers may be available for the FLETC's Center Advanced Training Programs held at the FLETC's training delivery points at Artesia, NM; Charleston, SC; Cheltenham, MD; and Glynco, GA. Attendance at Center Advanced programs is on a "space-available" basis. For a complete listing of FLETC Advanced Training Programs and registration information, please visit www.fletc.gov and select "training."

Cooperative Research and Development Agreements (CRADAs) are part of the national Technology Transfer Program, designed to assist Federal laboratories in leveraging taxpayer dollars. As a designated Federal laboratory and a member of the Federal Laboratory Consortium, the FLETC can provide personnel services, facilities, equipment, and other resources to support research and development that is beneficial to both the FLETC and the CRADA partner. The FLETC uses the CRADA program to establish partnerships for research and development in areas with potential to advance the nation's ability to train law enforcement personnel. The CRADA program can be used to identify and evaluate emerging technologies and training methodologies that can be incorporated into law enforcement and security training. For more information, see http://www.Federallabs.org or contact FLETC-CRADAProgramOffice@dhs.gov, 912-267-2591.

Office of Health Affairs (OHA)

The Office of Health Affairs (OHA) serves as the 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.

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; state and local agencies operate the system in their jurisdiction. 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 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 Biosurveillance Common Operating Picture (BCOP), a comprehensive electronic picture with assessments of current biological events, trends and their potential impacts on the Nation's homeland security. Access to the state and local BCOP (called Minerva) is available to public health, health care, agriculture, environment, and law enforcement personnel across the country at all levels of government.

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.

U.S. Immigration and Customs Enforcement (ICE)

U.S. Immigration and Customs Enforcement (ICE) 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 more than $5.7 billion dollars, primarily devoted to its two principal operating components - Homeland Security Investigations (HSI) and Enforcement and Removal Operations (ERO).

A Day in the Life of Enforcement and Removal Operations is a document that provides relevant and commonly requested statistics regarding ICE Enforcement and Removal Operations (ERO). Updated quarterly, it offers a snapshot of an average day's activities throughout ICE ERO. For more information, see http://www.ice.gov/doclib/news/library/factsheets/pdf/day-in-life-ero.pdf or you can access it online by visiting www.ice.gov,

Blue Campaign to Prevent Human Trafficking is the DHS human trafficking public outreach campaign. It provides critical human trafficking information to the public and provides a method for reporting suspected human trafficking activity. U.S. Immigration and Customs Enforcement (ICE) is the primary agency within DHS that fights human trafficking and conducts continuous outreach and training to U.S. and foreign law enforcement, non-governmental and international organizations, in order to foster awareness and provide information on the latest investigative techniques and victim assistance practices. The public is encouraged to report all suspicious activity to ICE at (866) DHS-2ICE (1-866-347-2423). Informational material on human trafficking is produced in a variety of languages, and is available to law enforcement, NGOs, and international organizations and includes the following: a public service announcement, human trafficking brochure in several languages, and human trafficking indicator wallet cards. See http://www.dhs.gov/topic/human-trafficking.

Document and Benefit Fraud Task Forces (DBFTF). ICE Homeland Security Investigations (HSI) leads 19 interagency task forces across the United States. Each DBFTF is comprised of Federal, state, and 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, Chicago, Dallas, Denver, Detroit, Houston, Los Angeles, Miami, New York, Newark, Orlando, Philadelphia, 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 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 Homeland Security Investigations Forensic Laboratory, the only federal crime laboratory dedicated to the forensic examination of travel and identity documents, and the HSI Cyber Crimes Center. For more information, please email

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

Forced Labor Resources. The ICE Office of International Affairs investigates allegations of forced labor in violation of the Tariff Act of 1930 (Title 19 USC §1307). To request more information or a copy of the A Forced Child Labor Advisory booklet and brochure, please contact: labor.iceforced@dhs.gov. 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; all pertinent facts known regarding the production of the product abroad. For the location of ICE foreign offices, please visit the ICE web site at http://www.ice.gov, click About Us, click International Affairs and select your country. ICE maintains a 24/7 hotline at (866) 347-2423 (from U.S. and Canada) or (802) 872-6199 (from any country in the world).

Human Rights Violators and War Crimes Center protects the public by targeting war criminals and those who violate human rights, including violators living both domestically and abroad. ICE investigators, intelligence analysts, and attorneys work with governmental and non-governmental agencies to accept tips and information from those who report suspected war criminals and human rights violators. Individuals seeking to report these abuses of human rights may contact the center at HRV.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, 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 a short video were developed by 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 Mutual Agreement between Government and Employers (IMAGE) Program is a joint government and private sector voluntary initiative that enhances employer compliance and corporate due diligence through training and sharing best practices regarding hiring practices. The goal of IMAGE is for the government to work with employers to develop a more secure and stable workforce and restore the integrity of the U.S. immigration system. For more information, see www.ice.gov/image or contact IMAGE@dhs.gov.

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, contact the center at BCSC@dhs.gov or 1-866-981-5332..

Online Detainee Locator System (ODLS) is a public system available on the Internet 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 Spanish, 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, see https://locator.ice.gov/odls/homePage.do

Project CAMPUS Sentinel is an outreach initiative established in April 2011 by ICE Homeland Security Investigations (HSI) directed toward academic institutions that are approved by HSI to enroll nonimmigrant students. The purpose of this outreach program is to build mutual partnerships between HSI Special Agent in Charge offices and Student and Exchange Visitor Program certified institutions. This exchange will enable HSI to detect and proactively combat student visa exploitations and address inherent national security vulnerabilities. For more information, contact CTCEU@DHS.gov.

Secure Communities and Civil Rights. Secure Communities is a critical tool for carrying out the immigration enforcement priorities ICE. To continue to improve the program, DHS is committed to addressing concerns that have been raised about its operation. This series of awareness briefings for state and local law enforcement is designed primarily for front line agency personnel and local leadership. Short videos, discussion guides, and job aids provide actionable information about the civil rights and civil liberties issues that may arise as ICE activates the Secure Communities Federal information-sharing capability in their jurisdictions. Topics include: what law enforcement needs to know, explaining Secure Communities to your community, immigration law protections for asylum seekers and for victims of crimes and human trafficking victims, working with non-English speakers, avoiding racial and ethnic profiling, contacting foreign consulates, misuse of Secure Communities as retaliation, use of ICE detainers, and civil rights and civil liberties complaints.
Available at:
www.ice.gov/secure_communities

Secure Communities: Get the Facts and Frequently Asked Questions. These two online resources provide explanations for and clarifications to many issues surrounding the Secure Communities initiative. For more information, see
http://www.ice.gov/secure_communities/get-the-facts.htm
http://www.ice.gov/secure_communities/faq.htm.

Secure Communities Training/Briefing Materials for State and Local Law Enforcement. These training/briefing materials include a series of modules; each module contains short viewable video and related materials such as fact sheets, discussion guides, web-based resources, and job aids. Although the modules will cover a number of topics and are designed to be presented as a series, law enforcement agencies may also present the materials in a variety of combinations to suit the needs of individual jurisdictions. The materials are designed for two distinct audiences: front line officers and law enforcement leadership (noted as the "Commander's packets"). For more information, see
http://www.ice.gov/secure_communities/crcl.htm.

Shadow Wolves. The ICE Homeland Security Investigations (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 United States 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 HSI Narcotics, Smuggling and BEST Unit in Washington, D.C. More information is available at http://www.ice.gov/news/library/factsheets/shadow-wolves.htm.

Student and Exchange Visitor Program (SEVP) was established in 2003 as the DHS front line effort to ensure that the student visa system is not exploited by those wishing to do harm to the United States. SEVP collects, maintains, and shares information in accordance with applicable laws and DHS policies so that only legitimate foreign students or exchange visitors gain entry to the U.S. The result is an easily accessible

information system that provides timely information to the Department of State, Department of Justice, and DHS Components.For more information, visit http://www.ice.gov/sevis/ or contact the SEVP Response Center at 703-603-3400.

The Cyber Crimes Center (C3), a component of Homeland Security Investigations (HSI), is responsible for delivering the highest quality cyber technical and investigative services to the field office and headquarters programs of ICE, in support of trans-border and infrastructure protection investigations. C3, through its Child Exploitation Investigations Unit, combats the exploitation of children, child pornography, international trafficking of children for sexual purposes, and child sex tourism by targeting individuals and organizations involved in these horrendous crimes. C3 addresses the widespread use of computers and digital devices through its Computer Forensics Unit. These devices have greatly increased the volume of data that ICE agents must examine during the course of an investigation. ICE agents now face a form of evidence that is highly volatile, mobile and capable of being encrypted by any user. C3's Cyber Crimes Unit is responsible for managing the cyber - component of traditional immigration and customs investigative categories. C3 special agents conduct and coordinate national level investigations where the Internet is used to further criminal activities across multiple areas. http://www.ice.gov/cyber-crimes/

The National Intellectual Property Rights Coordination Center (IPR Center) stands at the forefront of the U.S. government's response to global intellectual property (IP) theft. As a task force, the IPR Center uses the expertise of its member agencies to share information, develop initiatives, coordinate enforcement actions, and conduct investigation related to IP theft. Through this strategic interagency partnership, the IPR Center protects the public's health and safety, the U.S. economy, and the nation's war fighters. In 2010, Homeland Security Investigations (HSI) established the IP Theft Enforcement Teams (IPTETs) in each of the 26 HSI Special Agent in Charge offices around the country. The IPTETs use an informal task force approach where the IPR Center, its partner agencies and industry representatives can share best practices in combating IP theft with state and local law enforcement agencies and prosecutors. The IPR Center has completed 40 IPTET trainings across the country and continues to train state and local law enforcement, as well as federal and state prosecutors on a recurrent basis. The training promotes the task force platform that no one agency can combat this ever growing crime trend alone. Through the IPTET program, state and local law enforcement agencies become aware of the ways that IP theft attacks American businesses, finances organized crime and poses a threat to our public safety, our economy, and our war fighters. For more information, contact the IPR Center Global and Outreach Training Unit at iprcenteroutreach@dhs.gov.

Title 19 Cross-Designation. The HSI Title 19 Directive provides a mechanism for HSI to cross-designate state, county, local, municipal, and tribal law enforcement officers as "Customs officers" which serves to enhance the ability of HSI and DHS to work more cooperatively with our law enforcement partners. 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 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 HSI Narcotics, Smuggling and BEST Unit in Washington, D.C., or e-mail the unit at crossdes@fins3.dhs.gov. More information is available at http://www.ice.gov/customs-cross-designation.

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, see http://www.ice.gov/doclib/about/offices/osltc/pdf/tool-kit-for-prosecutors.pdf.

US Immigration and Customs Enforcements-Enforcement and Removal Operations (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. 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 ERO 101 in order to provide a more focused look at ICE ERO in the local area.

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 866-872-4973.

287(g) Fact Sheet provides information regarding the 287(g) program, one of ICE's top partnership initiatives. For more information, see http://www.ice.gov/news/library/factsheets/287g.htm.

Office of Intelligence and Analysis (I&A)

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

I&A works closely with Department Component intelligence organizations as well as state, local, tribal, 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 nation.

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 and sustain fusion center operations.

Counterintelligence Fundamentals Workshop (CIFWS). This is a joint training initiative offered by the DHS Counterintelligence Division (CIPD) and the FBI to provide a one-day, on-site workshop to fusion centers as a means of promoting counterintelligence awareness to the fusion centers. The CIFWS program is intended to familiarize the fusion center personnel with the possible intelligence collection threat directed against their facility, as well as the ability to recognize an elicitation attempt or recruitment pitch. Through brochures and other student materials distributed at the event, the CIFWS provides a reporting mechanism for SAR with a potential CI nexus. 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 required for this effort.

DHS Open Source Enterprise Daily Intelligence Reports. These reports provide open source information on multiple topics of interest. The following are currently available open source reports: the DHS Daily Digest Report, the DHS Daily Cyber Report, the DHS Weekly Human Trafficking and Smuggling Report, the DHS Daily Terrorism Report, and the DHS Daily Drug Trafficking and Smuggling Report. These reports may be accessed via the Homeland Security Information Network.

DHS-Single Point of Service (DHS-SPS). DHS-SPS serves as DHS Headquarters' central point for receiving and facilitating Requests For Information (RFIs) to the National Operations Center, I&A, DHS Components, and Federal partners. The DHS-SPS process 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. DHS-SPS processes all RFIs in a visible, transparent, and accountable manner to ensure they comply with existing

DHS statues, authorities, and policies.

DHS-SPS is available to all partners 24/7. State, local, tribal, and territorial partners should first reach out to their DHS deployed Operations or Intelligence officers prior to submitting an RFI to Headquarters DHS at SL_Support@hq.dhs.gov. Federal partners can submit their RFIs to DHS-RFI@hq.dhs.gov.

DHS Suspicious Activity Reporting (SAR) Initiative Management Group. DHS has engaged with the Nationwide SAR Initiative (NSI) in order to document and share terrorism-related SAR from DHS Components with other NSI participants. The DHS SAR Initiative Management Group (DSI MG) leads this engagement effort. The DSI MG facilitates the ability of DHS to produce SAR-related intelligence products and helps identify new trends and anomalies. The DSI MG helps each Component address unique policy, training and technological issues related to engagement with the NSI. Additionally, the DSI MG works with DHS Field Intelligence Officers to assist state and major urban area fusion centers in addressing their respective requirements related to NSI engagement. If you have any questions, comments or concerns related to the NSI engagement, please contact the DSI MG at 202-447-4008.

HSDN Resources for State and Local Law Enforcement. 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 SLE mission-related non-DHS information available via the DHS SLT SIPRNet Whitelist, which includes resources such as access to the NCTC 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.

I&A Homeland Security Intelligence Training Academy. The Mission Support Division (MSD) Intelligence Training Branch (ITB) designs, develops, assesses, and delivers intelligence training through a diverse set of training, education, and professional development programs to the DHS workforce and its Federal, state, local, tribal, territorial and private sector partners throughout the United States. If you have any further questions, please contact the I&A Registrar at 202-282 8866 or email the IAregistrar@dhs.gov.

Regional Analytic Advisor Plan (RAAP) provides information on the I&A Regional Analytic Advisor Plan (RAAP). The DHS/I&A established the RAAP to strengthen existing partnerships between DHS and State and Major Urban Area Fusion Center analysts and to enhance the exchange of expertise resident at each level.

RISSNET/BJA/ATIX - The Regional Information Sharing System (RISS) program is a network of regionally-aligned national information sharing initiatives designed to assist local, state, Federal, and tribal law enforcement and criminal justice agencies efforts in combating multi-jurisdictional criminal activities. RISS focuses on the support of investigations into terrorist activity, narcotics trafficking, gang and organized crime activity, human trafficking, identity theft, violent crime, and other related criminal activity. RISS maintains the Automated Trusted Information Exchange (ATIX) to provide the public and private sectors with interagency communication and information sharing capabilities. The POC for more information is Robert Nill at 202-282-8745.

National Protection & Programs Directorate (NPPD)

The National Protection & Programs Directorate (NPPD) leads the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure.

Active Shooter Awareness Training for Tenant Agencies. Federal Protective Service (FPS) offers awareness level instruction for occupants of Federal facilities regarding active shooter situations. The presentation covers the history of active shooter incidents; the evolution of police response tactics; reacting to an active shooter; facility lockdown procedures; what to do when law enforcement arrives; and employer responsibilities.

Training and Professional Development
703-235-6100
Robert.C.Marohn@ice.dhs.gov.

All-Hazards Communications Unit Leader (COML) Course is an Office of Emergency Communications (OEC)

Technical Assistance workshop 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 workshop is available to state and local law enforcement agencies as part of OEC Technical Assistance. For more information, see http://www.dhs.gov/files/programs/gc_1286979768422.shtm.

All-Hazards Communications Unit Technician (COMT) Course is an Office of Emergency Communications (OEC) Technical Assistance workshop that delivers introductory and refresher training for the Incident Command System COMT position. It introduces public safety professionals, and support staff, who wish to serve as a COMT utilizing various communications concepts and technologies. This workshop is available to state and local law enforcement agencies as part of OEC Technical Assistance. For more information, see http://www.dhs.gov/files/programs/gc_1286983307124.shtml.

Control Systems Security Program (CSSP) Cybersecurity Training is provided through an instructor-led introductory course for control system and IT professionals or a five-day advanced course which includes hands-on instruction in an actual control system environment. On-line introductory cybersecurity courses are also available. For more information, see http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications.pdf, or contact CSSP@dhs.gov.

Critical Infrastructure Protection and Resilience Training: *National Infrastructure Protection Plan (NIPP)* IS-(860.a) provides an overview of the public-private partnership, risk management framework, and information sharing approach used to integrate government and private sector into a national approach for infrastructure protection and resilience (http://training.fema.gov/EMIWeb/IS/is860a.asp) and (http://www.dhs.gov/files/programs/editorial_0827.shtm); and *Implementing Critical Infrastructure Protection Programs (IS-921)* addresses processes for informing partnerships, sharing information, managing risk, and ensuring continuous improvement.

Critical Infrastructure Security Awareness Training includes web-based independent study and classroom training and materials that address a variety of topics relevant to law enforcement. The Independent Study courses developed by the Office of Infrastructure Protection are available free of charge through the FEMA Emergency Management Institute. These courses include:

- *Workplace Security Awareness (IS-906)*, which provides training for a broad audience recognizing threats and improving security in the workplace (http://training.fema.gov/EMIWeb/IS/IS906.asp);
- *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 (http://training.fema.gov/EMIWeb/IS/IS907.asp); and
- 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 (http://training.fema.gov/EMIWeb/IS/IS912.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.

Current Cybersecurity Activity is a regularly updated summary of the most frequent, high-impact types of security incidents currently being reported to the US-CERT. For more information, see http://www.us-cert.gov/current/ or contact info@us-cert.gov or 888-282-0870.

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 and key resources (CIKR). The purpose of the CRR is to gather information regarding cybersecurity performance from specific CIKR in order to gain an understanding of the relationships and impacts of CIKR 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 18 CIKR sectors and within state governments and large urban areas. CSEP affords CIKR 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 18 Critical Infrastructure Sectors, state, local, tribal, and territorial governments. For more information, visit www.dhs.gov/xabout/structure/editorial_0839.shtm or contact CSE@dhs.gov.

Cybersecurity Information Products and Recommended Practices provide current cybersecurity information resources and recommend security practices to help industry understand emerging control systems, cybersecurity issues, and mitigate vulnerabilities. This information helps users reduce their exposure and susceptibility to cyber attacks and exploits. For a complete list and access to cybersecurity information products, visit http://www.us-cert.gov/control_systems/csdocuments.html. For more information, contact CSSP@dhs.gov.

Cybersecurity Public Trends and Analysis Report provides awareness of the cybersecurity trends as observed by the U.S. Computer Emergency Readiness Team (US-CERT). The analysis in this report is based on incident information that has been reported to US-CERT, incidents identified by US-CERT, and public/private sector information identified when correlating and analyzing the data. For more information, see http://www.us-cert.gov/reading_room/index.html#news or contact US-CERT at info@us-cert.gov or 888-282-0870.

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 the Office of Emergency Communications at oec@hq.dhs.gov or visit http://www.dhs.gov/xabout/structure/gc_1189774174005.shtm.

Explosive Detector Dog Program – The Federal Protective Service (FPS) Explosive Detector Dog (EDD) Program is a critical element of FPS' comprehensive security measures and supports strategic detection activities to clear identified areas of interest of explosive threats. The EDD 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. EDD teams are the most effective countermeasure available today for detection of explosives.
The EDD 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.
Chief, Canine Operations Branch
Uniformed Operations Division
703-235-6080
John.Hogan1@dhs.gov

Industrial Control System Cybersecurity Standards and References provides 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://www.us-cert.gov/control_systems/csstandards.html. For more information, contact CSSP@dhs.gov.

Information Technology Sector Risk Assessment (ITSRA) 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, see http://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf or contact ncsd_cipcs@hq.dhs.gov.

Mobile Command Vehicle Program - The Mobile Command Vehicle (MCV) program supports the Federal Protective Service (FPS) 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 United States 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 Mobile Command Vehicles 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 United States can be provided with service within one day.

Chief, Critical Incident Management Branch
Uniformed Operations Division
703-235-6080
Robert.Scott4@dhs.gov

National Cybersecurity Awareness Month (NCSAM) is held annually each October to help increase understanding of the threats and vulnerabilities facing the general public and the owners and operators of the Nation's Critical Infrastructure and Key Resources (CIKR). NCSAM also promotes other programs and initiatives within the Office of Cybersecurity and Communication (CS&C) that enhance the cyber resiliency of government and private sector cyber infrastructure. One of those programs is the Stop.Think.Connect.™ Campaign, which is a national public awareness effort initiated by President Obama's Cyberspace Policy Review to increase Americans' understanding of online safety. For more information please contact: cyberawareness@dhs.gov.

National Cybersecurity & Communications Integration Center (NCCIC) Operations Center reports 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 soc@us-cert.gov or 888-282-0870.

National Emergency Communications Plan (NECP) sets goals and identifies key national priorities to enhance governance, planning, technology, training, exercises, and disaster communications capabilities. The NECP

establishes specific national priorities to help state and local jurisdictions improve communications interoperability by adopting a series of goals and milestones that measure interoperability achievements over a period of years beginning in 2008, and ending in 2013. In order to successfully implement the NECP, increased collaboration between the public and private sector will be needed. As a result, the plan establishes specific initiatives and milestones to increase such collaboration. For more information, see http://www.dhs.gov/xlibrary/assets/national_emergency_communications_plan.pdf or contact the Office of Emergency Communications, oec@hq.dhs.gov.

National Interoperability Field Operations Guide (NIFOG) is a technical reference for radio technicians responsible for radios that will be used in disaster response applications, and for emergency communications. The NIFOG includes rules and regulations for use of nationwide and other interoperability channels, frequencies and channel names, and other reference material, formatted as a pocket-sized guide for radio technicians. The NIFOG can be accessed online at http://www.dhs.gov/files/publications/gc_1297699887997.shtm. For more information, contact the Office of Emergency Communications, oec@hq.dhs.gov.

OEC Interoperable Communications Technical Assistance Program (OEC/ICTAP) provides technical assistance (TA) 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 based on risk and capabilities, and it and supports all lanes of the SAFECOM Interoperability Continuum. Approximately 45 TA services are offered through the OEC TA Catalog. In addition, OEC/ICTAP pilots various offerings and employs its resources to support other DHS plans and programs such as the National Emergency Communications Plan (NECP). Three of these TA offerings are described in detail below. For more information, contact the Office of Emergency Communications at oec@hq.dhs.gov.

SAFECOM 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.
See http://www.safecomprogram.gov/grant/Default.aspx for more information, contact the Office of Emergency Communications at oec@hq.dhs.gov.

The SAFECOM Program works to improve multi-jurisdictional and intergovernmental communications interoperability. Its membership includes more than 70 members representing state and local 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. The site offers comprehensive information on topics relevant to emergency response communications and features best practices that have evolved from real-world situations. For more information, see http://www.safecomprogram.gov, or contact SAFECOM@dhs.gov.

SPCL-AUXCOMM (Auxiliary Communications). This OEC Technical Assistance workshop is designed for the Auxiliary Communicator (AuxComm) or group who provides emergency backup radio communications support to public safety agencies for planned or unplanned events at state and local levels. It is designed for AuxComm operators or groups who work with public safety and cross-disciplinary emergency response professionals. This workshop is available to state and local law enforcement agencies as part of OEC Technical Assistance.
For more information, see http://www.dhs.gov/files/training/gc_1287084689081.shtm.

The Federal Protective Service's (FPS) mission is to protect 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 carries out its mission by providing security planning; stakeholder engagement; law enforcement and information sharing services; and incident response.

The Information Technology Government Coordinating Council (IT GCC) provides a forum for interagency coordination, and partnership among DHS, NCSD, Federal, state, local, tribal and territorial governments with a role in protecting the IT Sector. For more information, please see: http://www.dhs.gov/files/committees/gc_1177096698216.shtm.

The NPPD Office of Infrastructure Protection offers an array of web-based and classroom courses, training materials, and tools that are designed to promote the knowledge and skills needed to implement critical infrastructure protection and resilience activities. The following sections highlight some of the programs that are relevant to the law enforcement community. More information about infrastructure protection training programs is available at: http://www.dhs.gov/training-programs-infrastructure-partners

The State, Local, Tribal and Territorial (SLTT) Cybersecurity Engagement Program fosters the relationships that protect our Nation's critical infrastructure and facilitates access to no-cost programs, resources, and services for SLTT governments. Governors and other appointed and elected SLTT 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 SLTT Cybersecurity Engagement Program, please send an email to SLTT@hq.dhs.gov.

U.S. Computer Emergency Readiness Team (US-CERT) Monthly Activity Summary provides monthly updates made to the National Cyber Alert System. This includes current activity updates, technical and non-technical alerts, bulletins, and tips, in addition to other newsworthy events or highlights. For more information, see http://www.us-cert.gov/reading_room/index.html#news; contact info@us-cert.gov 888-282-0870.

U.S. Computer Emergency Readiness Team (US-CERT) Security Publications provide subscribers with free, timely information on cybersecurity vulnerabilities, the potential impact of those vulnerabilities, and actions required to mitigate the vulnerability and secure their computer systems. For more information, see http://www.us-cert.gov/reading_room or contact info@us-cert.gov or 888-282-0870.

U.S. Computer Emergency Readiness Team (US-CERT) Vulnerability Notes Database includes technical descriptions of each vulnerability, as well as the impact, solutions and workarounds, and lists of affected vendors. For more information, see http://www.kb.cert.org/vuls or contact info@us-cert.govv or 888-282-0870.

United States Secret Service (USSS)

The mission of the United States Secret Service (USSS) 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.

Cell Phone Forensic Facility (Tulsa, OK). The Cell Phone 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 Cell Phone 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 U.S. Secret Service's fight against cybercrime. For more information, see www.secretservice.gov/TulsaCPFF.shtml. Requests for investigative assistance should be facilitated through your local Secret Service Field Office at www.secretservice.gov/field_offices.shtml.

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 CERT to state and local law enforcement agencies. For more information, see www.cert.org/forensics/tools.html

Cyber Intelligence Section (CIS). CIS collects, analyzes, and disseminates data in support of Secret Service investigations worldwide and generates new investigative leads based upon this intelligence. CIS leverages technology and information obtained through private partnerships to monitor developing technologies and trends in the financial payments industry for information that enhances 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. For more information, see www.secretservice.gov/ectf.shtml. Requests for investigative assistance should be facilitated through your local Secret Service Field Office at www.secretservice.gov/field_offices.shtml or contact your local ECTF.

eInformation Network. The Secret Service 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 US 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, see www.einformation.usss.gov.

Electronic Crimes Special Agent Program (ECSAP). ECSAP trained specialists conduct forensic examinations of computers, telecommunication devices, electronic organizers, scanners, and other electronic media located in field offices across the country and overseas. 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 www.secretservice.gov/field_offices.shtml or contact your local ECTF.

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 31 Secret Service ECTFs, to include London, England and Rome, Italy. Membership in the Secret Service ECTFs include approximately 300 academic partners; over 2,700 international, Federal, state, and local law enforcement partners; and over 3,100 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, see www.secretservice.gov/ectf.shtml.

Financial Crimes Enforcement Network (FinCEN). 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 United States 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 www.secretservice.gov/field_offices.shtml.

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 www.secretservice.gov/field_offices.shtml.

International Organized Crime Intelligence and Operations Center (IOC-2). The U.S. Department of Justice's International Organized Crime Intelligence and Operations Center (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 www.secretservice.gov/field_offices.shtml.

National Center for Missing and Exploited Children (NCMEC). The Secret Service supports the National Center for Missing and Exploited Children and local law enforcement agencies with its expertise in forensic photography, graphic arts, video productions, audio/image enhancement, voice identification, computerized 3D models, and video and audio tape duplication services. For more information, see http://www.secretservice.gov/partner_ncmec.shtml.

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 ten courses: Basic Investigation of Computer and Electronic Crimes Program (BICEP), Basic Computer Evidence Recovery Training (BCERT), Advanced Forensics Training (AFT), Network Intrusion Response Program (NITRO), Mobile Device Data Recovery, Online Social Networking, Computer Forensics in Court – Prosecutors, Computer Forensics in Court – Judges, Mobile Devices in Court – Prosecutors, and Point of Sales. Since its opening, the National Computer Forensics Institute has trained 1,142 state and local police investigators from over 500 agencies, 384 prosecutors and 141 judges from all 50 states and three U.S. Territories. 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. In FY2012, the NCFI trained 650 law enforcement, prosecutors and judges. For more information, see www.ncfi.usss.gov.

Transportation Security Administration (TSA)

The Transportation Security Administration (TSA) protects the Nation's transportation systems to ensure freedom of movement for people and commerce.

Joint Vulnerability Assessment (JVA) Training. The Office of Security Assessments (OSA), under the Office of Law Enforcement/Federal Air Marshal Service, Office of Security Services and Assessments 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 FY 2002, TSA took on the responsibility of conducting assessments from the FAA pursuant to the Aviation and Transportation Security Act (ATSA). When OSA conducts a JVA, it reaches out to, and works closely with, local law enforcement in order to identify vulnerabilities and recommends options to mitigate those vulnerabilities. OSA conducts JVA training as needed and it can be made available to local law enforcement upon request. For further information please email: OLEFAMSOSA@dhs.gov.

Law Enforcement Officer (LEO) Reimbursement Program provides partial reimbursement to state, local, or other public institutions/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 (LE) presence and support of passenger screening activities at U.S. commercial airports. For eligibility requirements please refer to CFDA 97.090 (www.cfda.gov).

Man-Portable Air Defense Systems (MANPADS) Awareness Training is a portable surface to air guided missile system designed to be carried by an individual. The Office of Security Assessments (OSA), under the Office of Law Enforcement/Federal Air Marshal Service, Office of Security Services and Assessments, conducts MANPADS Vulnerability Assessments 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. OSA also provides oversight and guidance on the development and implementation of MANPADS mitigation plans at the commercial airports.

OSA provides MANPADS awareness training to local law enforcement and other first responders. OSA 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 further information please email: OLEFAMSOSA@dhs.gov.

National Explosives Detection Canine Team Program (NEDCTP). TSA's NEDCTP prepares dogs and handlers to serve on the frontlines of America's War on Terror. These very effective, mobile teams provide an effective means to detect, deter, and prevent the introduction of explosives into the public transportation systems. Explosives Detection Canine Teams (EDCTs) are trained to work within the major transportation environments, i.e., aviation, maritime, mass transit surface and rail, etc., to detect various explosives odors. Screening 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. Just as important, EDCTs can quickly rule out the presence of dangerous materials in unattended packages, structures or vehicles, allowing the free and efficient flow of commerce. Departments or airports interested in participating in the NEDCTP may submit a letter of interest (on the official departmental letterhead) to the following address:

Chief, National Explosives Detection Canine Team Program
Federal Air Marshal Service
1900 Oracle Way Suite 400

Reston, VA 20190

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 our TSA website (http://www.tsa.gov/stakeholders/sensitive-security-information-ssi) or contact us directly at 571-227-3513 or SSI@dhs.gov.

TSA LEO Flying Armed Training Program. The FAMS Training Division (FAMSTD) 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 CFR 1544.219, Carriage of Accessible Weapons. The Law Enforcement Officers 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 Office of Law Enforcement/Federal Air Marshal Service, Office of Training and Workforce Programs, at LEOFA_TRN@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.