# DHS State and Local Law Enforcement Resource Catalog

Volume II-1

February 2014

Intentional Blank Page.  Please Continue to Next Page.

# Letter from the Office for State and Local Law Enforcement

February 24, 2014

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 Volume II-1*, we are pleased to announce a continuation of that effort.

The *DHS State and Local Law Enforcement Resource Catalog* is a one-stop shop for non-Federal law enforcement. This document summarizes and provides links to training, publications, newsletters, programs, and services available from across the Department to our law enforcement partners.

At DHS, we are continually developing new programs and resources that could be of assistance to state, local, and tribal law enforcement. If you cannot find what you are searching for in this catalog, please do not hesitate to contact 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. We hope this catalog is another one of those tools that will assist in your efforts to keep our communities safe, secure, and resilient.

Sincerely,

Office for State and Local Law Enforcement
Department of Homeland Security

# Office for State and Local Law Enforcement

## Overview

On the recommendation of the 9/11 Commission, Congress created the Office for State and Local Law Enforcement (OSLLE) in 2007 to lead the coordination of DHS-wide policies related to state, local, tribal, and territorial law enforcement's role in preventing, preparing for, protecting against, and responding to natural disasters, acts of terrorism, and other man-made disasters within the United States.

## Contact OSLLE


**Phone: 202-282-9545**

**Fax: 202-282-8306**

**Email: OSLLE@hq.dhs.gov**

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


## Responsibilities

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

***Helping to Build a Safe, Secure, and Resilient Nation***

# Table of Contents

**Letter from the Office for State and Local Law Enforcement ..... 3**
**Office for State and Local Law Enforcement (OSLLE) ..... 4**
**Department of Homeland Security Resources ..... 6**
Department-wide Resources..... 6
U.S. Citizenship and Immigration Services (USCIS)..... 7
USCIS Ombudsman (Ombudsman's Office) ..... 10
Office for Civil Rights and Civil Liberties (CRCL)..... 10
U.S. Coast Guard (USCG) ..... 14
U.S. Customs and Border Protection (CBP) ..... 15
Domestic Nuclear Detection Office (DNDO) ..... 16
Federal Emergency Management Agency (FEMA) ..... 20
Federal Law Enforcement Training Centers (FLETC) ..... 22
Office of Health Affairs (OHA) ..... 22
U.S. Immigration and Customs Enforcement (ICE) ..... 23
Office of Intelligence and Analysis (I&A) ..... 29
National Protection and Program Directorate (NPPD) ..... 30
**Privacy Office (PRIV) ..... 43
Science and Technology Directorate (S&T) ..... 44
U.S. Secret Service (Secret Service) ..... 45
Transportation Security Administration (TSA) ..... 48

## ***Department-Wide Resources***

**Blue Campaign to Fight Human Trafficking**. DHS is responsible for investigating human trafficking, arresting traffickers, and protecting victims. DHS also provides immigration relief to victims of human trafficking. The Blue Campaign is the unified voice for the DHS' efforts to combat human trafficking. Working in collaboration with law enforcement, government, non-governmental and private organizations, Blue Campaign strives to protect the basic right of freedom and to bring those who exploit human lives to justice. Increased awareness and training will lead to more tips to law enforcement, which results in more victims being identified. We cannot do this alone so please join us in the fight to end human trafficking. Visit the Blue Campaign website to learn about how we can work together and to learn about training, outreach materials, and victim assistance. Go to: www.dhs.gov/Bluecampaign. "Like" us on Facebook: www.facebook.com/bluecampaignOr, contact us at: BlueCampaign@hq.dhs.gov.

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

Specific Blue Campaign training products include:

- Web-based training about the indicators of human trafficking;
- Roll call videos explaining how available immigration relief for foreign victims provide a benefit to law enforcement;
- Handout material for law enforcement, non-governmental organizations, the Court, and first responders; and
- Public awareness posters and Public Service Announcements.

Visit www.dhs.gov/bluecampaign to access these and other training products.

**Homeland Security Information Network (HSIN)** is a national secure and trusted web-based portal for information sharing and collaboration between Federal, state, local, tribal, territorial, private sector, and international partners engaged in the homeland security mission. HSIN is made up of growing network of communities, called Communities of Interest (COI). COIs are organized by state organizations, Federal organizations, or mission areas such as emergency management, law enforcement, critical sectors, and intelligence. Users can securely share within their communities or reach out to other communities as needed. HSIN provides secure, real-time collaboration tools, including a virtual meeting space, instant messaging, and document sharing. HSIN allows partners to work together instantly, regardless of their location, to communicate, collaborate, and coordinate. For more information, please visit www.dhs.gov/HSIN.

**"If You See Something, Say Something™"**. The nationwide "If You See Something, Say Something™" public awareness campaign is a simple and effective program to raise public awareness of indicators of terrorism and terrorism-related crime, and to emphasize the importance of reporting suspicious activity to the proper local law enforcement authorities. The campaign was originally used by New York's Metropolitan Transportation Authority, which has licensed the use of the slogan to DHS for anti-terrorism and anti-terrorism crime related efforts. For more information about the initiative please go to: www.dhs.gov/ifyouseesomethingsaysomething.

**National Terrorism Advisory System (NTAS)** has replaced the Homeland Security Advisory System as our nation's primary domestic terrorism alerting resource. This new system more effectively communicates information about terrorist threats by providing timely, detailed information to the public, government agencies, first responders, airports and other transportation hubs, and the private sector. It recognizes that Americans all share responsibility for the nation's security, and should always be aware of the heightened risk of terrorist attack in the U.S. and

what they should do. After reviewing the available information, the Secretary of Homeland Security will decide, in coordination with other Federal entities, whether an NTAS Alert should be issued. For more information please go to http://www.dhs.gov/national-terrorism-advisory-system.

**Office of Inspector General (DHS OIG)**. DHS OIG conducts independent and objective criminal investigations, inspections and audits into fraud, waste, abuse, mismanagement, theft, or other criminal or noncriminal misconduct related to the funds, programs, or operations of DHS. DHS OIG derives its authority from the Inspector General Act of 1978, as amended, and the Homeland Security Act of 2002, and maintains a cadre of Criminal Investigators, Inspectors, and Auditors throughout the country who carry out the mission of promoting excellence, integrity, and accountability within DHS programs and operations.

DHS OIG operate a publicly accessible Complaint Hotline that DHS employees or members of the public can report criminal or noncriminal employee misconduct or inefficiencies related to DHS programs or operations. The Hotline encourages those wishing to make a report to use the online allegation form, call toll-free at 1 800-323-8603 or fax at 202-254-4292. For more information, including information regarding confidentiality, or to make a report, please visit: http://www.oig.dhs.gov/.

**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 frequently asked questions section that draws upon questions received by state and local law enforcement. For more information visit: http://www.dhs.gov/xlibrary/assets/dhs_u_visa_certification_guide.pdf.

## ***U.S. Citizenship and Immigration Services (USCIS)***

USCIS is the government agency that oversees lawful immigration to the United States. USCIS will secure America's promise as a nation of immigrants by providing accurate and useful information to our customers, granting immigration and citizenship benefits, promoting an awareness and understanding of citizenship, and ensuring the integrity of our immigration system.

**A Guide to Naturalization** contains information about the benefits and responsibilities of citizenship, an overview of the naturalization process, and eligibility requirements. See http://www.uscis.gov/natzguide.

**USCIS Citizenship Resource Center** is 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 skills to assist them during the naturalization interview and test. For more information, see http://www.uscis.gov/citizenship.

**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 United States. 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 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 webpages, 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 call the employers hotline at 888-464-4218/877-875-6028 (TTY) or the worker hotline at 888-897-7781 (TTY).

**Form I-9, Employment Eligibility Verification** is a form that U.S. employers must complete for each new employee. 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 United States. 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; Guidance 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).

**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.

**Law Enforcement Support Operation Unit**. USCIS's Fraud Detection and National Security (FDNS) Directorate has developed a centralized operation to administer the S Visa Program and facilitate the issuance of notional (cover) immigration documents.

The S visa program is available for aliens who possess "critical reliable information" regarding criminal activity, who are willing to share their information with a U.S. agency or court and whose presence in the U.S. 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's Public Engagement Division (PED)** seeks to focus on open, candid, and

constructive collaboration with community stakeholders at all levels. PED is dedicated to coordinating and directing agency-wide dialogue with external stakeholders to actively collaborate and maintain open and transparent communication and to seek feedback regarding policies, priorities, and organizational performance reviews. The goal of the division is to provide information and invite feedback to inform USCIS's work. See http://www.uscis.gov for more information or contact Public.Engagement@dhs.gov.

**USCIS Resources** offers a variety of resources including customer guides, videos, 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 to 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.

**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, local, tribal and territorial 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 T or U visa nonimmigration status. The investigating or prosecuting law enforcement agency does not make the request to USCIS on the victim's behalf. Once the victim requests T or U visa status, USCIS reviews the request and all submitted evidence to determine eligibility. Other related resources include:

- **Law Enforcement Fact Pages**. USCIS has a fact sheet entitled "Immigration Relief for Victims of Human Trafficking and Other Crimes" for law enforcement officials. The fact sheet answers frequently asked questions on the immigration relief options for victims of human trafficking and other crimes through DHS (ICE and USCIS). The sheet covers Continued Presence and U and T visas

- **Immigration Relief Brochure**. USCIS has a brochure entitled "Immigration Options for Victims of Crime" covering the basics of Violence Against Women Act (VAWA) self-petitions and T and U visas aimed for law enforcement and health care providers.

- **In-Person and Web-Based Training**. USCIS offers in person and web-based presentations for law enforcement on T and U visas. If interested contact USCIS at: T-U-VAWATraining@dhs.gov.

These resources (available in several languages) and more information on T and U visas can be found at www.uscis.gov/humantrafficking and http://www.dhs.gov/blue-campaign.



*Substantive edits since last update
**New addition to Resource Catalog
2/24/14

## ***U.S. Citizenship and Immigration Services Ombudsman (Ombudsman's Office)***

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

**Send Your Recommendations to the Ombudsman's Office**. The Ombudsman is dedicated to identifying systemic 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. 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 online 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.

## ***Office for Civil Rights and Civil Liberties (CRCL)***

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

CRCL is also responsible for assuring that the Department's federally-assisted programs comply with various civil right laws, including but not limited to Title VI of the Civil Rights Act of 1964, as amended; Title IX of the Education Amendments of 1972, as amended; and the Rehabilitation Act of 1973, as amended.

**Civil Rights Requirements in Federally-Assisted Programs**. CRCL provides resources, guidance, and technical assistance to recipients of DHS financial assistance on complying with Title VI of the Civil Rights Act of 1964 (Title VI) Section 504 of the Rehabilitation Act of 1973, and related statutes.

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

**Common Muslim American Head Coverings and Common Sikh American Head Coverings Posters** provide guidance to



*Substantive edits since last update
**New addition to Resource Catalog
2/24/14

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. *Available from*: CRCL's website: http://www.dhs.gov/civil-rights-and-civil-liberties-institute.

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

**Community Roundtables**. CRCL leads, or plays a significant role, in regular roundtable meetings across the country in over 14 U.S. cities. These roundtables bring exceptionally diverse demographic communities together with Federal, state, local, tribal, and territorial government representatives. Issues discussed range from immigration and border issues to civil rights issues in aviation security. CRCL also conducts roundtables with young leaders of diverse communities. For more information please contact communityengagement@hq.dhs.gov.

**Countering Violent Extremism (CVE) training**. In accordance with the White House's National Security Strategy and the DHS Homeland Security Advisory Council 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*: Email 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 CVE, cultural awareness, and counterterrorism training. *For more information*: Please visit CRCL's website: http://www.dhs.gov/civil-rights-and-civil-liberties-institute.

**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 non-governmental organizations, 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 emailing 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 DHS. 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 U.S. Attorney who is a practicing Muslim; a member of the National Security Council who is a practicing Muslim; a scholar of Islamic studies; and a civil rights attorney who advocates on issues of concern to Arab American and Muslim American communities. The training assists law enforcement officers and other personnel who interact with Arab and Muslim Americans, as well as individuals from Arab or Muslim communities in the course of their duties. For more information, contact crcltraining@dhs.gov or visit http://www.dhs.gov/civil-rights-and-civil-liberties-institute.

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

**Privacy, Civil Rights & Civil Liberties Fusion Center Training Program**. The Implementing Recommendations of the 9/11 Commission Act requires that DHS support fusion centers by providing training on privacy, civil rights, and civil liberties. As a result, CRCL and the DHS Privacy Office have partnered with the DHS Office of Intelligence & Analysis, State and Local Program Office, and the DOJ Bureau of Justice Assistance to deliver this training program. The program has included: A website Resource center found at



*Substantive edits since last update
**New addition to Resource Catalog
2/24/14

www.it.ojp.gov/PrivacyLiberty; a training of Privacy/Civil Liberties Officers program; a technical assistance program; and an on-site training program.

Topics covered include: civil rights and civil liberties basics and red flags (how to spot potential issues and incorporate safeguards into your procedures); privacy fundamentals (how to integrate your privacy policy and recognize and respond to a privacy incident); cultural tactics for intelligence and law enforcement professionals (covers frequently encountered misconceptions and stereotypes and addresses policies against racial or ethnic profiling); and First Amendment issues in the information sharing environment (covers considerations when fusion centers may encounter constitutionally protected activities, such as freedom of speech, demonstrations, petitions for redress, etc.). Fusion centers and their liaison officer networks have the option of choosing additional topics to create a customized agenda. Technical assistance is also available.
*Duration*: Full-day (8 hours) but can be customized to shorter sessions.
For more information, email FusionCenterTraining@dhs.gov.

**Quarterly Non-governmental Organization (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 U.S. Immigration and Customs Enforcement have collaborated to create a series of downloadable awareness briefings for state, local, tribal, and territorial 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 designed to provide actionable information to state and local law enforcement about civil rights and civil liberties issues and 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, limited English proficiency, unlawful retaliation by private actors, protecting victims and witnesses of crime, outreach, 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 United States. This video was developed by the DOJ Community Relations Service and reproduced by DHS.
*Duration*: 10 minutes.
*Available from*: CRCL's website: http://www.dhs.gov/civil-rights-and-civil-liberties-institute. This site also offers a transcript and limited resources and glossary.
*Available from*: DVD can be ordered from the CRCL by emailing crcltraining@dhs.gov.

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



*Substantive edits since last update
**New addition to Resource Catalog

Available at: http://www.it.ojp.gov/PrivacyLiberty.

## ***United States Coast Guard (USCG)***

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

Surface platforms consist of boats and larger cutters. Vessels under 65 feet in length are classified as boats and usually operate near shore on inland waterways and from cutters. Craft include: Motor Lifeboats; Medium and Small Response Boats; special purpose response boats; port security boats; Aids to Navigation boats; and a variety of smaller, non-standard boats including rigid hull inflatable boats. Sizes range from 64-foot in length down to 12-foot. Cutters are basically any commissioned USCG vessel 65 feet in length or greater, having adequate accommodations for crew to live onboard. Cutters usually have one or more rigid hull inflatable boats onboard. Polar Class icebreakers also carry an Arctic Survey Boat and Landing Craft. The USCG cutter fleet ranges from a 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 and C-144 Ocean Sentry turboprops) operate from large and small Air Stations. Rotary wing aircraft (H-65 Dolphin and HH-60 Jayhawk helicopters) operate from flight-deck equipped Cutters, Air Stations, and Air Facilities.

USCG Deployable Specialized Forces (DSF) provides additional teams and resources such as Maritime Safety and Security Teams (11), Port Security Units (8), Tactical Law Enforcement Teams (2), Maritime Security Response Team (1), National Strike Force and Regional Dive Lockers (2). DSF teams are capable of worldwide deployment via air, ground or sea transportation in response to changing threat conditions and evolving Maritime Homeland Security mission requirements. Core capabilities include: Enhanced Law Enforcement Boardings; Waterside Security/Force Protection; Landside Security/Force Protection; Port Security; Subsurface Operations; Chemical, Biological, Radiological, Nuclear and Enhanced Conventional Weapons (CBRNE) Detection and Identification; Disaster Response; Environmental Response; Deployable Incident Management; Advanced Planning; and multiple supporting capabilities.

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

**USCG Maritime Information eXchange ("CGMIX")** makes USCG maritime information available to the public on the internet in the form of searchable databases. Much of the information on the CGMIX web site comes from the USCG's Marine Information for Safety and Law Enforcement (MISLE) information system. For more information see http://cgmix.uscg.mil/.

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

***USCG Sector Command Centers**. Given USCG mission diversity, asset readiness status

and ongoing operations, the main avenue for proper and expeditious USCG asset mobilization requests are through USCG Sector Command Centers. There are 37 USCG Sector Commands throughout the U.S. and U.S. territories:

| Sector Command Centers | | |
|---|---|---|
| **Sector Name** | **Location** | **24/7 Contact** |
| Anchorage | Anchorage, AK | 907-271-6769 |
| Baltimore | Baltimore, MD | 410-576-2525 |
| Boston | Boston, MA | 617-223-5757 |
| Buffalo | Buffalo, NY | 716-843-9525 |
| Charleston | Charleston, SC | 843-740-7050 |
| Columbia River | Warrenton, OR | 503-861-6211 |
| Corpus Christi | Corpus Christi, TX | 361-939-6393 |
| Delaware Bay | Philadelphia, PA | 215-271-4940 |
| Detroit | Detroit, MI | 313-568-9560 |
| Guam | Santa Rita, Guam | 671-355-4824 |
| Hampton Roads | Portsmouth, VA | 757-638-6641 |
| Honolulu | Honolulu, HI | 808-842-2600 |
| Houston-Galveston | Houston, TX | 713-678-9011 |
| Humboldt Bay | McKinleyville, CA | 707-839-6113 |
| Jacksonville | Atlantic Beach, FL | 904-564-7511 |
| Juneau | Juneau, AK | 907-463-2990 |
| Key West | Key West, FL | 305-292-8727 |
| Lake Michigan | Milwaukee, WI | 414-747-7182 |
| LA-Long Beach | San Pedro, CA | 310-521-3801 |
| Lower Mississippi | Memphis, TN | 901-521-4804 |
| Long Island | New Haven, CT | 203-468-4401 |
| Miami | Miami, FL | 305-535-4472 |
| Mobile | Mobile, AL | 251-441-6211 |
| New Orleans | New Orleans, LA | 504-365-2533 |
| New York | Staten Island, NY | 718-354-4353 |
| North Bend | North Bend, OR | 541-756-9210 |
| North Carolina | Wilmington, NC | 910-343-3880 |
| Northern New | South Portland, ME | 207-767-0303 |
| Ohio Valley | Loiusville, KY | 502-779-5424 |
| Puget Sound | Seattle, WA | 206-217-6002 |
| San Diego | San Diego, CA | 619-278-7057 |
| San Francisco | San Francisco, CA | 415-399-3530 |
| San Juan | San Juan, PR | 787-289-2041 |
| Sault Ste Marie | Sault Ste Marie, MI | 906-635-3233 |
| Southeastern New England | Woods Hole, MA | 508-457-3211 |
| St Petersburg | St Petersburg, FL | 727-824-7506 |
| Upper Mississippi | St Louis, MO | 314-269-2463 |

## ***U.S. Customs and Border Protection (CBP)***

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

**Carrier Liaison Program** provides standardized training and assistance to international air carriers related to admissibility and fraudulent document detection in order to encourage carrier compliance with U.S. immigration laws. For more information about the Carrier Liaison Program, visit 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 focus on outreach to community stakeholders and provide fact-based information regarding the CBP mission, functions, authorities, and responsibilities. Border Community Liaisons nationwide can be assessed through the CBP State, Local, Tribal Liaison Office at 202-325-0775 or by emailing CBP-STATE-LOCAL-TRIBAL-LIAISON@cbp.dhs.gov.

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

**CBP Laboratories and Scientific Services** coordinates technical and scientific support to all CBP and DHS-wide trade and border protection activities including laboratory analysis for trade enforcement and product safety, forensic services for criminal investigations, and 24/7 telephonic access to scientific resources for technical case adjudication. For more information, visit http://www.cbp.gov/xp/cgov/newsroom/fact_sheets/border/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. ESTA applications may be submitted at any time prior to travel, though it is recommended travelers apply when they begin preparing travel plans. ESTA applicants are required to pay a $14.00 fee with their 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 (IPR)**. CBP's IPR Help Desk provides information on IPR border enforcement procedures

and receives allegations of IPR infringement. Questions regarding IPR enforcement at U.S. borders and information on IPR infringing goods that may be entering the U.S. can be directed to the IPR Help Desk at 562-980-3119 ext. 252, or via email at jpr.helpdesk@dhs.gov

**Missing or Late International Travelers**. Information regarding reported missing or late international travelers can be obtained from the nearest port of entry. For a list of ports, 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 of human trafficking 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 persons 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 (DOS) Office of Children's Issues to prevent the international abduction of children involved in custody disputes or otherwise against the published order of the court. If you are concerned about the international travel of a child, please contact the DOS Office of Children's Issues at PreventAbduction@state.gov or the 24 hour hotline 888-407-4747.

***State, Local and Tribal Liaison (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 cbp-state-local-tribal-liaison@cbp.gov or 202-325-0775.

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

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

**Visa Waiver Program (VWP)** enables citizens and nationals from 36 countries to travel to and enter the U.S. for business or visitor purposes for up to 90 days without obtaining a visa. For more information about the Visa Waiver Program, please visit http://www.cbp.gov/xp/cgov/travel/id_visa/business_pleasure/vwp/.

## ***Domestic Nuclear Detection Office (DNDO)***

DNDO is a jointly staffed office within DHS. DNDO is the primary entity in the U.S. government for implementing domestic 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, tribal, 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.



*Substantive edits since last update
**New addition to Resource Catalog
2/24/14

***Equipment Test Results**. Federal, state, local, and tribal agencies intending to purchase radiological and nuclear detection equipment are strongly encouraged to consider only instruments that have been independently tested by accredited laboratories and have demonstrated conformity with the applicable American National Standards Institute/ Institute of Electrical and Electronics Engineers (ANSI/IEEE) N42 standards. Manufacturers offering new equipment for consideration should be asked to provide evidence of independent testing for compliance with these standards. DNDO has resources described below that are available to assist Federal, state, local, tribal, and territorial entities in selecting the right radiological and nuclear 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 radiological and nuclear detection procurement decisions of Federal, state, local, tribal, and territorial entities. Examples of test reports include: Anole Test Campaign Report for handheld, backpack, and mobile systems (available on COI and Responder Knowledge Base); Bobcat Test Campaign Report for commercial-off-the-shelf and prototype personal radiation detectors; Crawdad and Dolphin Test Campaign Reports for boat-mounted detection systems (available upon request); Gryphon Test Campaign Report for aerial detection systems. Several of these test campaign results are available on the Preventative Radiological/Nuclear Detection (PRND) COI and the Responder Knowledge Base (RKB) at https://www.llis.dhs.gov/knowledgebase, while others may be requested by contacting DNDO at DNDO.INFO@hq.dhs.gov.

**Exercises**. DNDO provides assistance in developing, designing, and conducting exercises that are compliant with the Homeland Security Exercise and Evaluation Program 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 JAC, located within DNDO, provides awareness of the Global Nuclear Detection Architecture (GNDA) and provides technical support to Federal, state, local, and tribal authorities. Utilizing the Joint Analysis Center Collaborative Information System (JACCIS), the JAC facilitates radiological and nuclear alarm adjudication from detection events and consolidates and shares information and databases.

GNDA Awareness is achieved by establishing and maintaining links to detectors and access to Nuclear Regulatory Commission and Agreement State Material Licensing Data. GNDA Awareness also depends upon non-time critical requirements such as access to historical data on all detection events (illicit and legitimate) and access to information about commerce and related radiological and nuclear infrastructure that affects detection assets and response protocols.

JACCIS provides a process for Federal, state, 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 (NIEM) standardized message types that can be provided by these internet connected systems: radiological and nuclear alarms, an inventory of radiological and nuclear assets, radiological and nuclear sites, and radiological and nuclear 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)**. DNDO's MDDP utilizes trailer-based Mobile Detection Deployment Units (MDDUs) outfitted with an extensive suite of radiation detection equipment and command and control capabilities. These assets are modeled after, maintained and deployed by the Department of Energy (DOE) National Nuclear Security Administration (NNSA) Radiological Assistance Program (RAP). The MDDUs are deployed regionally across the U.S. and are maintained through an agreement with DOE RAP Teams. MDDUs serve as readily deployable radiation detection equipment packages and provide equipment augmentation and "surge" detection capability for Federal, state, local, and tribal stakeholders for special events, enhanced operations and intelligence-driven searches. 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 DNDO with the concurrence of DOE First Responder programs. Additional information concerning the MDDP can be directed to DNDO.SLA@hq.dhs.gov. Requests to use MDDU assets should be emailed to DNDO_MDDU_Request@hq.dhs.gov.

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

***PRND Program Management Handbook with Commercial Vehicle Inspection, 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 commercial vehicle inspections, small maritime vessel operations, and special events. This handbook provides guidance for the administration of a domestic PRND program and is intended to assist with 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 web portal at https://auth.dhs.gov/oam/hsinl

ogin or by contacting DNDO at DNDO.SLA@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 detection capability based on risk factors and the likelihood of encountering illicit radiological and nuclear material. The CDF is based on lessons learned provided by Federal, state, local, and tribal 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 that supports the Screening, Search, and Detection core capability and can be leveraged to support investment justifications. A CDF Calculator is also available to assist jurisdictions with identifying recommended levels of radiological and nuclear detection capability quickly and easily. The CDF and supporting resources are available on the PRND Community of Interest web portal (see below) or by contacting DNDO at DNDO.SLA@hq.dhs.gov.

**Radiological and Nuclear Detection (RND) Community of Interest (COI)**. DNDO's RND 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 RND COI, submit a request by email to DNDO with a message subject line of: "DNDO RND COI HSIN Access Request" to the address: PRND_COI@hq.dhs.gov.

***Radiological and Nuclear Detection (RND) Program Assistance**. DNDO works with Federal, state, local, tribal, and territorial government policy makers, program managers, and operational administrators to design, implement, and sustain a radiological and nuclear detection program. DNDO's RND Program Assistance includes the development of Concepts of Operation, Standard Operating Procedures, Multiyear Training and Exercise Plan, Sustainment Plan, Table Top Exercise, and the sharing of lessons learned and best practices.

The program goal is to prevent the deployment of a radiological or nuclear terrorist weapon against the interior of the U.S. by establishing a sustainable capability among Federal, state, local, tribal, and territorial agencies and emergency responders to detect and report unauthorized radiological and/or nuclear materials out of regulatory control within their jurisdictions/regions.

***Securing the Cities (STC) Program**. The STC 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 GNDA and encourage participants to sustain the base nuclear detection program over time. There are three phases to the program; In 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. In Phase II, STC provides additional resources to enhance



*Substantive edits since last update
**New addition to Resource Catalog
2/24/14

detection, analysis, communication, and coordination to better integrate state and local capabilities with Federal government activities and the GNDA beyond Phase I. Finally, in Phase III, STC 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 DNDOSTC@hq.dhs.gov.

**Training**. DNDO training strives to provide quality products and support to develop, enhance, and expand radiological and nuclear detection capabilities in support of the GNDA. Together with other Federal partners, the DNDO training program provides technical review, evaluation, and continual developmental improvement of the radiological and nuclear detection training curriculum to increase the operational detection capabilities of Federal, state, local, tribal, and territorial agencies to detect and interdict radiological and nuclear 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 radiological and nuclear detection training for over 27,000 law enforcement, first responder personnel, and public officials through Fiscal Year 2013.

Radiological and 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. For more information, visit 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)***

FEMA's mission is to support our citizens and first responders to ensure that as a nation we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards.

**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.

**First Responder Training.** 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 include citizen and community preparedness, response to terrorist events, and recovery operations for disasters of at shapes and sizes.

- FEMA's Center for Domestic Preparedness (CDP), is DHS's only Federally-chartered Weapons of Mass



*Substantive edits since last update
**New addition to Resource Catalog
2/24/14

Destruction (WMD) training center. The interdisciplinary resident and nonresident training courses at CDP promote a greater understanding among the diverse responder disciplines: Emergency Management, Emergency Medical Services, Fire Service, Governmental Administrative, Hazardous Materials, Healthcare, Law Enforcement, Public Health, Public Safety Communications, and Public Works.

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

The curricula is structured to meet the needs of this diverse nation and our wide range of first responders with an emphasis on separate organizations working together in all-hazards emergencies to save lives and protect property. The NTED Course Catalog provides valuable information courses. The First Responder Training information can be found at www.firstrespondertraining.gov

**Office of Protection and National Preparedness** contributes to the development and implementation of preparedness doctrine that reaches Federal state, local, tribal, and territorial emergency management communities, as well as non-government entities and the private sector. The guidance and doctrine includes Preparedness (Non-Disaster) Grants, National Preparedness Guidelines, National Incident Management System, and National Planning Frameworks.

- Within its National Preparedness Directorate, the National Integration Center examines emerging technologies, develops state and local planning guidance, and supports resource typing and the credentialing of emergency response personnel.

- Within its National Continuity Programs, FEMA provides guidance and tools for continuity at all levels of government and communications systems. Continuity of Operations is an effort within departments and agencies to ensure that Primary Mission Essential Functions continue to be performed during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies. The Integrated Public Alert and Warning System (IPAWS) provide law enforcement officials with resources for training, information, and guidance on integrating IPAWS Common Alerting Protocol compliant emergency and incident management tools with existing alerts and warning systems, as well as the availability of grants to update alert and warning infrastructures.

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

**Preparedness (Non-Disaster) Grant** funding in the form of competitive grants to enhance the capacity of state, local, tribal, and territorial emergency responders to prevent, respond to, and recover from a weapon of mass destruction, terrorism incident involving chemical, biological, radiological, nuclear, explosive devices, and cyber-attacks. For more information on how to find and apply for grants visit www.fema.gov/preparedness-non-disaster-grants or www.Grants.gov.



*Substantive edits since last update
**New addition to Resource Catalog

**Responder Knowledge Base (RKB)** serves as a resource to the state, local, tribal, and territorial 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, equipment specifications, related certifications and applicable standards, test reports, the InterAgency Board Standardized Equipment List, and other information. For more information visit: http://www.rkb.us.

## ***Federal Law Enforcement Training Centers (FLETC)***

***Contact Information:***

***Federal Law Enforcement Training Centers**

**Address:** 1131 Chapel Crossing Road, Bldg. 2200, Glynco, GA 31524

**E-mail:** stateandlocaltraining@dhs.gov

**Phone:** 800-743-5382 or 912-267-2345

**Hours of Operation**: 8 a.m. – 5 p.m. EST (Mon-Fri)

**T**he FLETC offers advanced and specialized law enforcement training in a variety of topics through the State, Local, and Tribal Division (SLD) to state, local, and tribal law enforcement officers throughout the U.S. and Indian country. The programs SLTD delivers are developed with the advice, assistance and support of Federal, state, local, and tribal law enforcement agencies and are continuously updated to ensure relevance to today's issues. They are conducted at selected venues throughout the country provided by a local law enforcement agency or at one of FLETC's training delivery points which are located in Artesia, NM; Charleston, SC; Cheltenham, MD; and Glynco, GA. Tuition assistance may be available to state, local, and tribal officers, but attendance is on a "space-available" basis. For further information, to consult the registration procedure and/or for a complete listing of FLETC's advanced and specialized training programs please visit www.fletc.gov and select "training" or you may contact SLTD by e-mail at stateandlocaltraining@dhs.gov or by phone at 800-743-5382.

**The FLETC Online Campus** is a secure online learning management system (LMS) developed by the FLETC in support of the law enforcement learning environment. The Online Campus currently offers 165 professionally developed interactive online courses available for access by U.S. sworn, vetted law enforcement officers and agents. Online Campus registration and access to course materials is provided through the Regional Information Sharing System (RISS), and requires law enforcement officers to complete the ATIX Application form. Please visit http://www.fletc.gov/elp-splash/ for more information.

## ***Office of Health Affairs (OHA)***

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

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

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

**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)***

ICE's primary mission is to promote homeland security and public safety through the criminal and civil enforcement of Federal laws governing border control, customs, trade, and immigration. The agency has an annual budget of more than $5.7 billion dollars, primarily devoted to its two principal operating components - Homeland Security Investigations (HSI) and Enforcement and Removal Operations (ERO).

**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.

**A Day in the Life of Enforcement and Removal Operations** is a document that provides relevant and commonly requested statistics regarding ICE 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.

**Border Enforcement Security Task Force (BEST)**. In response to increased crime along the Southwest border, ICE HSI, in partnership with U.S. Customs and Border Protection (CBP), and other Federal, state, local, tribal, territorial, and international law enforcement officials expanded its ongoing Border Crimes Initiative by creating BEST, a multi-agency initiative. There are currently 35 BEST units comprised of approximately 1,000 members representing 100 law enforcement agencies working jointly to investigate transnational criminal activity along the Southwest Border, Northern Border, and major seaports. 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/BEST.htm.

***Cyber Crimes Center (C3)**, a component of ICE HSI, was established in 1997 for the purpose of combating crimes committed on, or facilitated by, the Internet. C3 brings together highly technical assets dedicated to conducting trans-border criminal investigations of Internet-related crimes within the HSI portfolio of immigration and customs authorities. C3 is responsible for identifying and targeting any cybercrime activity in which HSI has jurisdiction. C3's current mission is fourfold: (1) Keep pace with emerging computer technology and Internet processes; (2) Proactively use these new technologies to combat criminal activity and address vulnerabilities created by the Internet; (3) Disseminate to field offices and the worldwide law enforcement and intelligence organizations the most current trends, risks, procedures, lessons learned, and investigative leads; and (4) Support investigations into Internet criminal activities and vulnerabilities with state-of-the-art cyber investigative methods and forensic techniques. For more information, see http://www.ice.gov/cyber-crimes/.

***Cyber Crimes Unit (CCU)** is responsible for managing the cyber component of traditional immigration and customs investigative -categories. CCU special agents provide support for international level investigations. HSI's cyber investigations primarily focus on international economic crime, Internet-facilitated smuggling and money laundering, the illegal acquisition and proliferation of export controlled technology and data, the theft and sale of digital intellectual property, and child exploitation crimes.

***Document and Benefit Fraud Task Forces (DBFTF)**. ICE HSI leads 19 interagency task forces across the United States. Individual task forces can be comprised of Federal, state, and/or local law enforcement partners working together to combat immigration document and benefit fraud, as well as related criminal violations. DBFTF locations include Atlanta, Baltimore, Boston, 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 HSI Forensic Laboratory, the only Federal crime laboratory dedicated to the forensic examination of travel and identity documents, and the HSI Cyber Crimes Center (C3). For more information, see http://www.ice.gov/document-benefit-fraud/.

***Forced Labor Program**. ICE HSI investigates allegations of forced labor in violation of the Tariff Act of 1930 (Title 19 USC §1307), relating to the illegal importation of goods mined, manufactured, or produced, wholly or in part, through the use of forced labor, prison labor, and/or indentured labor under penal sanctions. When contacting ICE to report instances of forced labor, please provide as much detailed information and supporting documentation as possible, including the following: a full statement of the reasons for the belief that the product was produced by forced labor and that it may be or has been imported into the United States; a detailed description of the product; and all pertinent facts known regarding the production of the product abroad. Reports may be sent to ICE.ForcedLabor@ice.dhs.gov. ICE also maintains a 24/7

hotline at 866- 347-2423 (from U.S. and Canada) or 802-872-6199 (from any country in the world), that can take this information.

***HSI Forensic Laboratory** (HSI-FL) provides a broad range of forensic, intelligence, and investigative support to HSI, ICE, DHS, and many other U.S. and foreign law enforcement agencies. The HSI-FL is accredited by the American Society of Crime Laboratory Directors / Laboratory Accreditation Board (ASCLD/LAB). Forensic disciplines include questioned documents, fingerprints, and chemistry. Additionally, the HSI-FL provides intelligence alerts, reference material on travel and identity documents, and fraudulent document detection training. The HSI-FL oversees the HSI Evidence Recovery Team Program. See www.ice.gov/hsi-fl for additional information.

**HSI Tip Line**. The HSI Tip Line and the HSI Online Tip Form serve as conduits for individuals to report suspected criminal activity. Managed by the agency's Tip Line Unit, the tip line and tip form receive and record information from the general public and law enforcement 24/7/365. Investigative leads are forwarded to 7,000 special agents in 200 cities nationally and to 47 countries around the world. Unit members reach out to duty agents to relay time sensitive information and have the capability to customize questions to meet the needs of national enforcement priorities. Phone toll free 866-347-2423 from the U.S. and Canada, or from any country in the world phone 802- 372-6199. www.ice.gov/tips

**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 HSI 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.

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

**ICE 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.

****Law Enforcement Information Sharing Initiative (LEISI)** facilitates the sharing of DHS sensitive but unclassified law enforcement information with other federal, tribal, state, local, and international law enforcement agencies. LEISI provides the electronic Law Enforcement Information Sharing Service (LEIS Service) that other law enforcement agencies can utilize to query records pertaining to ICE



*Substantive edits since last update
**New addition to Resource Catalog
2/24/14

criminal subjects and ICE and CBP immigration violators. For more information, contact LEISI at DHS-LEISI@ice.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 866-981-5332.

***National Intellectual Property Rights Coordination Center (IPR Center)** stands at the forefront of the U.S. government's response to global intellectual property (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, ICE HSI established the State and Local Engagement Program to educate and foster better relationships between state and local law enforcement and HSI field offices. The State and Local Engagement Program leverages the resources of the IPR Center to deliver IPR-focused training to state and local law enforcement. The IPR Center and the International Anti-Counterfeiting Coalition Foundation, with the support of local HSI field offices, delivers IP-focused hands-on training. The training seminars provide a forum for Federal, state, local law enforcement and prosecutors to share best practices and develop relationships with industry representatives, which is crucial in the investigation and prosecution of IP theft violations. These trainings help state and local law enforcement to become aware of the ways IP theft attacks American businesses and finances organized crime. Additionally, the IPR Center supports the National Association of Attorneys General and the National White Collar Crime Center, who also deliver IP-focused training to state and local law enforcement officers. For additional information on available resources and training please contact the National Intellectual Property Rights Coordination Center, Global Outreach and Training Unit at iprcenteroutreach@dhs.gov.

**The Office of State, Local and Tribal Coordination (OSLTC)** is responsible for building and improving relationships and coordinating partnership activities for multiple stakeholders – including state, local, and tribal governments, as well as law enforcement agencies/groups. OSLTC's vision is to provide stakeholders with a clear understanding of ICE's components, structure, mission, goals, and responsibilities.

For additional information, visit http://www.ice.gov/about/offices/leadership/osltc/.

****Operation Community Shield Task Forces (OCSTF)**. Operation Community Shield is the HSI anti-gang initiative that combines ICE's expansive statutory and administrative enforcement authorities to combat the growth and proliferation of transnational criminal street gangs, prison gangs, and outlaw motorcycle gangs throughout the United States in cooperation with our Federal, state, local, tribal, and foreign law enforcement partners. OCSTFs officially align HSI with our partners to enhance intelligence gathering and information sharing, exploit 21st century law enforcement technology, and further capitalize on our worldwide presence to combat these global criminal networks and mitigate the threats they pose to the public safety and national security of the United States and



*Substantive edits since last update
**New addition to Resource Catalog

other countries.

**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 HSI directed toward academic institutions that are approved by ICE HSI to enroll nonimmigrant students. The purpose of this outreach program is to build mutual partnerships between ICE HSI Special Agent in Charge offices and Student and Exchange Visitor Program certified institutions. This exchange enables ICE HSI to detect and proactively combat student visa exploitations and address inherent national security vulnerabilities. For more information, contact CTCEU@DHS.gov.

**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 and http://www.ice.gov/secure_communities/faq.htm.

**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 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 HSI Shadow Wolves are Native American Tactical Officers assigned to the Tohono O'odham Nation in Arizona to enforce immigration and customs laws and regulations. This reservation contains 2.8 million acres of land and includes a 75-mile-long stretch

of the U.S. border with Mexico. The Shadow Wolves use their unique language and tracking skills to interdict and investigate contraband and have assisted law enforcement with the investigation of kidnappings, the deaths of illegal aliens, sexual assaults, missing children, and any reports of border violence. The Shadow Wolves have traveled to the Blackfeet Indian Reservation and the Bay Mills Chippewa Indian Reservation to share their expertise.

Additionally, the Shadow Wolves have conducted training with the U.S. Department of Defense in several of the former Soviet Republics to teach the ancient art of tracking to combat nuclear proliferation from the former Soviet Republics. For additional information, please contact 800-973-2867 and ask to speak with the Unit Chief for the 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 United States. 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.

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

**Trade Transparency Unit (TTU)** provides world-renowned subject matter expertise on trade-based money laundering through investigative, analytical, and intelligence case support to ICE HSI domestic and international offices, and to our U.S. and international law enforcement partners. The TTU's unique capabilities are enhanced by international cooperation agreements with foreign partners that seek the ability to share trade data which can be compared through HSI's Data Analysis & Research for Trade Transparency System (DARTTS), which allows for the detection of trade and financial discrepancies that are indicative of trade-based money laundering and other financial crimes. For more information,

contact the TTU at TTU@ice.dhs.gov or 1-800-973-2867.

**U.S. Immigration and Customs Enforcement – Enforcement and Removal Operations 101 (ERO 101)** is a PowerPoint presentation compiled to introduce ICE ERO and its program offices. Though the slides themselves are not accessible to the public, the presentation can be delivered by any field office upon request. 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.

## ***Office of Intelligence and Analysis (I&A)***

I&A is a member of the national Intelligence Community (IC) and ensures that information related to homeland security threats is collected, analyzed, and disseminated to the full spectrum of homeland security partners in the Department, at Federal, state, local, tribal, and territorial levels, in the private sector, and in the IC.
I&A works closely with Department Component intelligence organizations as well as state, local, tribal, territorial, and private sector entities to ensure non-traditional streams of information are fused with traditional IC sources to provide a complete assessment of threats to the homeland.

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

I&A is the Executive Agent for coordinating Federal support for state and major urban area fusion centers. It also leads the Department's information sharing efforts. I&A works to solidify productive and collaborative relationships with its partners to enhance information sharing. This collaboration and coordination is bolstered by the placement of I&A intelligence officers at each of the state and major urban area fusion centers, providing direct intelligence support to key State, local, tribal, and territorial partners, and private sector partners.

**Counterintelligence Fundamentals Workshop (CIFWS)** is a joint training initiative offered by the DHS Counterintelligence Division (CIPD) and the Federal Bureau of Investigation (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. 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 daily and weekly reports provide open source information on multiple topics of interest to facilitate a greater understanding of the nature and scope of threats and hazards to the homeland. They are provided to Federal, state, local, tribal, territorial, and private sector officials to aid in the identification and development of appropriate actions, priorities and follow-on measures. These reports may be accessed via the

Homeland Security Information Network.

**DHS-Single Point of Service (DHS-SPS)** serves as DHS Headquarters' 24x7 central ingest point for receiving, tracking, and facilitating Operational and Intelligence Requests For Information (RFIs) to Federal, state, local, tribal, and territorial partners. The DHS 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. Before submitting an RFI to SPS, Federal and DHS Component partners should route their RFIs through their respective headquarters to ensure they have visibility. State and local partners should work through their Fusion Center(s) (via their deployed I&A Intelligence Officers) to verify all local resources have been exhausted.

DHS-SPS representatives can be contacted at:

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

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

**HSDN Resources for State and Local Partners**. Appropriately-cleared state and local personnel assigned to Fusion Centers are granted access to Secret-level network resources via the Homeland Secure Data Network (HSDN). These resources include intelligence products from I&A that are hosted on HSDN, as well as a range of SLE mission-related non-DHS information available via the DHS SLT SIPRNet Whitelist, which includes resources such as access to the National Counterterrorism Center Current portal for counter-terrorism information, the DEA portal for counternarcotics intelligence, and a number of Department of Defense sites including cybersecurity, counterterrorism, intelligence, and counternarcotics information.

**I&A Homeland Security Intelligence Training Academy (ITA)**. The I&A Homeland Security ITA's mission is to advance students' knowledge, skills, and abilities through the creation and dissemination of Homeland Security intelligence training enabled by professional staff and instructors, innovative learning programs, and modern facilities. For information regarding the ITA's course offerings, please contact the I&A Registrar at 202-282-8866 or email the IAregistrar@dhs.gov.

**Regional Analytic Advisor Plan (RAAP)**. 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.

## ***National Protection and Programs Directorate (NPPD)***

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

### ***ACTIVE SHOOTER PREPAREDNESS RESOURCES***

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

***Active Shooter Awareness Training for Tenant Agencies**. NPPD's 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. For more information contact Training and Professional Development at 703-235-6100 or Robert.C.Marohn@hq.dhs.gov.



*Substantive edits since last update
**New addition to Resource Catalog

***BIOMETRIC IDENTITY MANAGEMENT***

**Office of Biometric Identity Management (OBIM) Biometric Support Center (BSC)** provides expert fingerprint identification services in support of DHS's Automated Biometric Identification System, which contains the fingerprints of over 160 million individuals. The BSC supports fingerprint search requests including those of unknown individuals (e.g., deceased subjects, cold cases). The BSC operates 24 hours a day/7 days a week. For additional information, contact the BSC at afis@dhs.gov.

***CHEMICAL SECURITY***

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

For more information, visit www.dhs.gov/chemicalsecurity. To report a facility you believe may not be in compliance with the regulation, call the DHS CFATS Tip Line, at 877-394-4347 (877-FYI 4 DHS).

***COUNTER-IMPROVISED EXPLOSIVE DEVICE (IED) PROGRAMS AND RESOURCES***

****Counter-IED Awareness Cards & Posters** are available to public and private sector security partners to enhance awareness of IED threats, protective measures for mitigating vulnerabilities, and information on reporting suspicious activity. Available products include information on black powder, black powder substitutes, smokeless powder, hazardous chemicals, peroxide products, suspicious purchasing behavior, suicide bomber/active shooter awareness, suspicious behavior for hotels and lodgings, precursor chemicals, and suspicious purchasing behavior for online retailers. For more information, contact OBP@hq.dhs.gov.

**Counter- IED & Risk Mitigation Training** is offered by OBP to build counter-IED core capabilities and enhance awareness of terrorist threats to critical infrastructure amongst FSLTT, and private sector entities. Coordinated through State Homeland Security Officials and training offices, the courses educate participants on strategies for detecting and mitigating threats. Available courses are listed below; to request training, contact your local Protective Security Advisor (PSA) or email OBP@hq.dhs.gov for additional information.

- **Bomb-making Materials Awareness Program (BMAP) Training** is an outreach initiative, developed in partnership with the Federal Bureau of Investigation (FBI), to increase public and private sector awareness of homemade explosives by promoting private sector point-of-sale awareness and suspicious activity reporting to prevent misuse of explosive precursor chemicals, powders, and components commonly used in IEDs. BMAP training is designed for first responders with counterterrorism outreach responsibilities and builds knowledge of IED threats, home made explosives, and bomb-making materials. The course also provides guidance and materials to help participants conduct outreach to industries and businesses within their jurisdictions in order to strengthen prevention opportunities. BMAP training events are designed to accommodate 75 participants. For more information, please contact OBP@hq.dhs.gov.

- **Bomb Threat Management Workshop** improves the ability of critical infrastructure owners, operators, and security managers to manage IED threats by highlighting specific safety precautions associated with explosive incidents and bomb threats.

The workshop reinforces an integrated approach that combines training, planning, and equipment acquisition to maximize available resources for bomb threat management. Public and private sector representatives knowledgeable in regional emergency management procedures are encouraged to attend. This four-hour course can accommodate 50 participants. For more information, please contact OBP@hq.dhs.gov.

- **IED Counterterrorism Workshop** enhances participant understanding of the IED threat, surveillance detection methods, and soft target awareness. The workshop also covers awareness and prevention activities that reduce vulnerabilities, as well as collaborative information sharing resources to improve first responder and public and private sector counter-IED preparedness. This eight-hour workshop can accommodate 250 participants. For more information, please contact OBP@hq.dhs.gov.

- **IED Search Procedures Workshop** builds awareness of IED threats, prevention measures, and planning protocols to detect IEDs by reviewing specific search techniques. This workshop increases knowledge of counter-IED principles and techniques among first responders and public and private sector security partners tasked with IED search and response protocols. This eight-hour course can accommodate 40 participants. For more information, please contact OBP@hq.dhs.gov.

- ***Protective Measures Course** builds awareness and understanding of the IED threat, terrorist planning cycle, and indicators of suspicious activity. Participants, including critical infrastructure staff tasked with increasing the security posture of a facility or event, learn about facility vulnerability analysis, counter-IED protective measures, and strategies which can be utilized to mitigate risk and reduce vulnerabilities within their unique sectors.. This two-day course can accommodate 25participants. For more information, please contact OBP@hq.dhs.gov.

- **Surveillance Detection Course for Law Enforcement and Security Professionals** provides instruction on how to detect hostile surveillance by exploring surveillance techniques, tactics, and procedures from a hostile perspective. These skills enhance counter-IED capabilities of law enforcement and security professionals to detect, prevent, protect against, and respond to IED threats. This three-day course can accommodate 25 participants. For more information, please contact OBP@hq.dhs.gov.

- **Vehicle-borne IED (VBIED) Detection Course** improves participants' ability to successfully inspect for, detect, identify, and respond to a VBIED. Instruction covers the VBIED threat; explosive effects; IEDs; and vehicle inspections, enabling participants to better detect, deter, and protect against the illicit use of explosives. The course is designed for first responders and public and private sector security staff tasked with inspecting vehicles for explosives, dangerous goods, or contraband. This eight-hour course can accommodate 20 participants. For more information, please contact OBP@hq.dhs.gov.

***Multi-Jurisdiction Improvised Explosive Device Security Planning (MJIEDSP)** program is a systematic process that fuses counter-improvised explosive device (IED) education, capability analysis, training, and planning to enhance counter-IED capabilities in high-risk jurisdictions to enhance IED prevention, protection, and response capabilities. The DHS Office for Bombing Prevention (OBP) works closely with each MJIEDSP community to assist in identifying roles, responsibilities, and capability gaps, and provides expertise on



*Substantive edits since last update
**New addition to Resource Catalog

planning and operational requirements for IED incident response, as outlined in the National Preparedness Goal and expressed through FEMA's Core Capabilities. For more information, contact OBP@hq.dhs.gov.

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

***Technical Resource for Incident Prevention (TRIP*wire*)** is the DHS 24/7 online, collaborative, information sharing network for bomb squad, first responders, military personnel, government officials, intelligence analysts, and security professionals to increase awareness of evolving terrorist IED tactics, techniques, and procedures, as well as incident lessons learned and counter-IED preparedness information. Developed and maintained by OBP, the system combines expert analyses and reports with relevant documents, images, and videos gathered directly from terrorist sources to help users anticipate, identify, and prevent IED incidents. TRIP*wire* is also regularly used to share critical information with our Federal, state, local, tribal, territorial (FSLTT) and private sector security partners during periods of heightened alert or following IED related incidents. To register, visit http://tripwire.dhs.gov.

- ***DHS-DOJ Bomb Threat Guidance Brochure** is designed to help site decisionmakers of commercial facilities respond to a bomb threat in cooperation with first responders and other stakeholders to ensure actions are conducted in a systematic and orderly manner. Includes pre-threat planning guidance, including the development of an Emergency Toolkit, and provides procedural guidelines and instructions if a bomb threat is received, or for conducting a threat assessment. .The brochure is available to registered TRIP*wire* users or upon request at OBP@hq.dhs.gov.

- ****DHS Bomb Threat Procedures Checklist** provides a quick reference tool to help public and private sector partners respond to a bomb threat. It provides basic procedural guidelines and a checklist to document important information if a bomb threat is received over the phone. For more information, please contact OBP@hq.dhs.gov.

- **DHS-DOJ Bomb Threat Stand-off Card** was jointly developed by OBP and the FBI to provide standardized, national explosive threat categorization and response guidelines with stand-off distances that can be applied by public safety bomb squads and law enforcement. For more information, contact OBP@hq.dhs.gov.

- ***FiRST* Application**, or First Responder Support Tools Application, was developed by OBP and DHS Science & Technology Directorate in collaboration with the private sector. The application allows first responders to quickly define safe stand-off distances around a potential bomb location, calculate rough damage and injury contours, suggest appropriate roadblocks, and identify other nearby facilities of concern using their smartphones and laptop computers. DHS bomb stand-off data is considered sensitive and only made available to those who register the application using a .*gov*, .mil, or .*us* email address. For additional



*Substantive edits since last update
**New addition to Resource Catalog
2/24/14

information on downloading the application, please visit: http://www.ara.com/products/first.

- ***Protective Measures Guidance** is provided by OBP to assist public and private sector security partners in establishing secure environments with IED threat preparation and planning to bolster security posture and IED incident mitigation. Information includes pre-event and incident response planning, measures for reducing vulnerabilities, suspicious behavior awareness, and reporting protocols to address various IED threat scenarios, such as mass gatherings and homicide/suicide bombers. These documents are available to registered TRIP*wire* users or upon request at OBP@hq.dhs.gov.

- **VBIED Identification Guide: Parked Vehicles** is a reference card for use by law enforcement and security professionals to identify indicators of a possible VBIED. The card is intended for distribution to personnel conducting security patrol or perimeter and access control duties during major events. The product is available to registered TRIP*wire* users or upon request at OBP@hq.dhs.gov.

- **Vehicle Inspection Guide & Video**. The Vehicle Inspection Guide (VIG) was developed for use by law enforcement, bomb squads, HAZMAT teams, other emergency and public government service organizations, and professional security personnel involved with vehicle inspection. The Vehicle Inspection Video is designed to complement the VIG by providing demonstrations of vehicle search techniques. An electronic copy of the Guide and Video are available to registered TRIP*wire* users. For more information, contact OBP@hq.dhs.gov.

***CYBERSECURITY***

**COBALT Information Sharing Compartment** is a web-based information sharing compartment within the US-CERT Portal that provides actionable cybersecurity information to the broader community of cybersecurity professionals. The National Cybersecurity and Communications Integration Center (NCCIC) shares cyber threat indicators and advisory information through Cobalt with public and private partners, including sector-specific stakeholders. For more information and to request access, email NCCIC_Partnership @hq.dhs.gov.

**Control Systems Security Program – 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.

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



*Substantive edits since last update
**New addition to Resource Catalog

**Cybersecurity Evaluation Program (CSEP)** conducts voluntary cybersecurity assessments across all 16 critical infrastructure sectors and within state governments and large urban areas. CSEP affords critical infrastructure and key resources sector participants a portfolio of assessment tools, techniques, and analytics, ranging from those that can be self-applied to those that require expert facilitation or mentoring outreach. The CSEP works closely with internal and external stakeholders to measure key performances in cybersecurity management. The Cyber Resiliency Review is being deployed across all 16 critical infrastructure sectors, state, local, tribal, and territorial governments. For more information, visit www.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 NCCIC@us-cert.gov or 888-282-0870.

**Emergency Services Sector-Cyber Risk Assessment (ESS-CRA)**. The 2012 ESS-CRA is the first ESS-wide cyber risk assessment that analyzes strategic cyber risks to ESS infrastructure. The ESS-CRA process provides a national-level risk profile that ESS partners can use to prioritize how they spend resources and where to focus training, education, equipment investments, grant requests, and further study. The risk assessment consisted of seven evaluation sessions to solicit input from ESS subject-matter experts. Each scenario evaluated threats, vulnerabilities, and consequences to ESS cyber infrastructure. Stakeholders chose scenarios based on what would have the widest impact - the scenarios likely to affect the most disciplines at a time. The final ESS-CRA report includes a risk profile showing how the scenarios would affect each discipline, and the operational impact. Cyber risks to each discipline are ranked from high to low in terms of likelihood and consequence. The assessment approach is not intended to be guidance for individual entity's risk management activities. Instead, by increasing the awareness of risks across the public and private sector domains, the ESS-CRA serves as a foundation for ongoing national-level collaboration to enhance the security and resilience of the ESS disciplines. If you have any questions about the ESS Cyber Risk Assessment, please send an email to ESSTeam@hq.dhs.gov.

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

If an organization believes it is experiencing a cyber event on control systems/critical infrastructure please call 1-877-776-7585 or e-mail ICS-CERT at ics-cert@hq.dhs.gov. To report ICS software vulnerability please visit http://www.kb.cert.org/vuls/html/report-a-vulnerability/ and



*Substantive edits since last update
**New addition to Resource Catalog
2/24/14

fill out the Vulnerability Reporting Form. Please follow the directions to encrypt to the CERT Pretty Good Privacy key in order to protect sensitive, non-public vulnerability information.

**Industrial Control System Cybersecurity Standards and References** 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://ics-cert.us-cert.gov/Standards-and-References. For more information, contact ics-cert@dhq.dhs.gov.

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

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

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

**Multi-State Information Sharing and Analysis Center (MS-ISAC)** seeks to improve the overall cybersecurity posture of state, local, tribal, and territorial partners. Collaboration and information sharing among members, private sector partners, and DHS are the keys to success. State, local, tribal, and territorial Government representatives who believe they are experiencing a cyber event of any kind, please call 1-866-787-4722 for the 24x7 MS-ISAC Security Operations Center, or by visiting http://msisac.cisecurity.org/about/incidents and clicking on the "Report an Incident" button.

**National Coordinating Center for Telecommunications (NCC)** continuously monitors national and international incidents and events that may impact emergency communications. Incidents include not only acts of terrorism, but also natural events such as tornadoes, floods, hurricanes, and earthquakes. To receive information on the NCC, please e-mail NCCIC@hq.dhs.gov and ask to be added to the NCC distribution list. The National Cybersecurity & Communications Integration Center will review and grant access based upon authorization by the NCC approval authority.

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



*Substantive edits since last update
**New addition to Resource Catalog

**National Cybersecurity Awareness Month (NCSAM)** held annually each October, is the culmination of yearlong Stop.Think.Connect.™ Campaign cybersecurity activities. Through events and other initiatives, NCSAM helps increase understanding of the cyber threats and vulnerabilities facing the general public and the owners and operators of the Nation's critical infrastructure. Each week of the month covers a pressing cybersecurity theme, typically including a week devoted to cybercrime. For more information see http://www.dhs.gov/national-cyber-security-awareness-month or contact the Campaign at stopthinkconnect@dhs.gov.

**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.

**The Stop.Think.Connect.™ Campaign** is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. Initiated by President Obama's Cyberspace Policy Review, the Department of Homeland Security leads the Campaign in partnership with the National Cyber Security Alliance and the Anti-Phishing Working Group. Law enforcement agencies and other organizations can receive cybersecurity materials and collaborate with other members by joining the Cyber Awareness Coalition of government agencies or the National Network of non-profit groups. For more information see http://www.dhs.gov/stopthinkconnect or contact the Campaign at stopthinkconnect@dhs.gov.

**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; or contact NCCIC@us-cert.gov, or call 888-282-0870.

**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 NCCIC@us-cert.gov or 888-282-0870.

**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 NCCIC@us-cert.govv or 888-282-0870.

***FEDERAL PROTECTIVE SERVICE RESOURCES***

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

**Explosive Detector 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



*Substantive edits since last update
**New addition to Resource Catalog

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. For more information contact the Chief of the Canine Operations Branch Uniformed Operations Division at 703-235-6080 or John.Hogan1@dhs.gov.

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

FPS has eight MCVs located at regional offices around the country, as well as four SUV-based mobile communications vehicles, known as "Rabbits." The Rabbits provide most of the same communications capabilities as the MCVs, but lack the command and control space and workstations. The Rabbits afford a rapid deployment capability, as well as the ability to navigate tight spaces and unimproved roads, which allows for the projection of communications services into areas that would otherwise be inaccessible. The Rabbits are designed to extend their electronic footprint into buildings of opportunity so that they can be rapidly converted into command posts with the full communications services. Strategic locations around the country ensure that each vehicle has a 750 mile "first due" response radius and that any area of the continental U.S. can be provided with service within one day. For more information, please contact the Chief of the Critical Incident Management Branch, Uniformed Operations Division at 703-235-6080 or Robert.Scott4@dhs.gov.

### *INFRASTRUCTURE SECURITY AND RESILIENCE TRAINING AND RESOURCES*

**Critical Infrastructure Asset Protection Technical Assistance Program** is a weeklong course designed to assist state and local law enforcement, first responders, emergency management, and other homeland security officials understand the steps necessary to develop and implement a comprehensive critical infrastructure protection program in their respective jurisdictions through the facilitated sharing of best practices and lessons learned. This includes understanding processes, methodologies, and resources necessary to identify, assess, prioritize, and protect critical infrastructure assets, as well as those capabilities necessary to prevent and respond to incidents, should they occur. Through a partnership with the National Guard Bureau, the U.S. Army Research, Development and

Engineering Command, and NPPD's Office of Infrastructure Protection (IP), this service also provides Web-based and instructor-led training on Protected Critical Infrastructure Information and the use of the Automated Critical Asset Management System (ACAMS) and DHS geospatial viewers. See http://www.dhs.gov/cikr-asset-protection-technical-assistance-program. For more information, contact IP's Training Team at TrainingHelp@hq.dhs.gov.

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

- *Critical Infrastructure Protection: Achieving Results through Partnership and Collaboration* (IS-913) provides an overview of the elements and processes that develop and sustain successful critical infrastructure protection partnerships and collaborations. It covers the skills and tools needed to achieve critical infrastructure protection and resilience through partnership and collaboration. http://training.fema.gov/EMIWeb/IS/courseOverview.aspx?CODE=IS-913.a

- *Implementing Critical Infrastructure Protection Programs* (IS-921.a) addresses processes for informing partnerships, sharing information, managing risk, and ensuring continuous improvement. https://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=IS-921.a

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

- *Critical Infrastructure Security: Theft and Diversion – What You Can Do* (IS-916) is designed for critical infrastructure employees and stakeholders, and provides information and resources available to identify threats and vulnerabilities to critical infrastructure from theft and diversion of critical resources, raw materials, and products that can be used for criminal or terrorist activities. The course also identifies actions that can be taken to reduce or prevent theft and diversion. http://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=IS-916

- *Protecting Critical Infrastructure Against Insider Threats* (IS-915) provides guidance to critical infrastructure employees and service providers on how to identify and take action against insider threats to critical infrastructure. It is designed for all personnel and service providers who are associated with critical infrastructure. http://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=IS-915

- *Retail Security Awareness: Understanding the Hidden Hazards* (IS-912), which is designed to make persons involved in commercial retail operations aware of the actions they can take to identify and report suspicious purchases or thefts of products that actors could use in terrorist or other criminal activities http://training.fema.gov/EMIWeb/IS/IS912.asp



*Substantive edits since last update
**New addition to Resource Catalog
2/24/14

- *Surveillance Awareness: What You Can Do* (IS-914) provides training on actions that can be taken to detect, deter, and report suspicious activities associated with adversarial surveillance. It is designed for individuals with little to no physical or operations security experience. http://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=is-914

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

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

**Homeland Infrastructure Threat and Risk Analysis Center** provides infrastructure consequence analysis and prioritization capabilities to DHS, government, and private sector stakeholders. HITRAC experts analyze the effects of risk mitigation actions in many forms, including strategic threat and risk analysis; modeling and simulation; and analytic support to Department decisionmakers and security partners before, during, and after incidents. HITRAC, I&A, and FEMA also provides risk analysis tradecraft training to State Fusion Centers. For HITRAC products available on The Homeland Security Information Network, see https://hsin.dhs.gov/ci/iir/hitrac/Pages/default.aspx. For access to risk analysis tradecraft training call (202) 282-8866 or e-mail FusionCenter Support@hq.dhs.gov
For questions or requests, please email risk@hq.dhs.gov.

**Homeland Security Information Network – Critical Infrastructure (HSIN-CI)**

HSIN-CI provides secure networked information sharing covering the full range of critical infrastructure interests. Validated critical infrastructure partners are eligible for HSIN-CI access.

- The NICC posts content from a variety of internal and external sources that is available to all Critical Infrastructure (CI) partners, including incident situation reports, threat reports, impact modeling and analysis, common vulnerabilities, potential indicators, and protective measures.
- The NICC combines current high-interest incidents and events on the HSIN-CI "front page" to enable easy access to relevant information.
- Individual sectors and sub-sectors self-manage more specific portals within HSIN-CI where smaller communities of participants receive and share relevant information for their particular information needs.
- HSIN-CI also includes capabilities to facilitate multiple types of information sharing and coordination, including suspicious activity reporting, webinars, shared calendars, etc.
- To ensure broad sharing of essential information, the NICC also receives and provides information via other HSIN portals.

To request HSIN-CI access, submit the following to HSIN.Helpdesk@hq.dhs.gov:

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

For questions regarding HSIN-CI access, please contact the NICC.

**Infrastructure Protection Gateway** serves as the single interface through which DHS mission partners can access a large range of integrated IP tools and data to conduct comprehensive vulnerability assessments and data analysis. This, in turn, enables homeland security partners to quickly

identify relevant vulnerability and consequence data in support of event planning and response efforts. The IP Gateway provides various data collection, analysis, and response tools into one system, streamlining access to IP's tools and datasets by leveraging a single user registration, management, and authentication process. Highlights of the IP Gateway include the ability to access: a selection of physical and cyber vulnerability tools and security surveys; a consolidated library of critical infrastructure data, assessments and reports; integrated data visualization and mapping tools to support complex data analysis; and situational awareness tools to support special event and incident planning and response activities. For more information visit: www.dhs.gov/criticalinfrastructure, or contact the Help Desk: iicd@hq.dhs.gov or 1-866-844-8163.

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

To contact: nicc@hq.dhs.gov or 202–282–9201.

***PUBLIC SAFETY AND EMERGENCY COMMUNICATIONS***

**All-Hazards Communications Unit Leader (COML) Course** is an NPPD's 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, contact OEC at oec@hq.dhs.gov.

**Auxiliary Communications** 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, contact the OEC at oec@hq.dhs.gov.

**Emergency Communications Guidance Documents and Methodologies** are stakeholder-driven guidance documents and methodologies to support emergency responders across the Nation as they plan for and implement emergency communications initiatives. These resources identify and promote best practices for improving statewide governance, developing standard operating procedures, managing technology, supporting training

and exercises, and encouraging use of interoperable communications. Each is available publicly and is updated as needed. Examples include the Public Safety Communications Evolution Brochure, Establishing Governance to Achieve Statewide Communications Interoperability, and the Formal Agreement and Standard Operating Procedure Template Suite. For more information, contact the Office of Emergency Communications at oec@hq.dhs.gov or visit www.publicsafetytools.info.

**National Emergency Communications Plan (NECP)** sets goals and identifies key national priorities to enhance governance, planning, technology, 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 is vital. 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 at oec@hq.dhs.gov.

**OEC Interoperable Communications Technical Assistance (TA) Program** provides technical assistance at no cost to all levels of state, local, and tribal law enforcement to support interoperable communications solutions and practices. This assistance is offered annually through Statewide Interoperability Coordinators based on risk and capabilities, and it and supports all lanes of the SAFECOM Interoperability Continuum. Approximately 60 TA services are offered through the OEC TA Catalog. In addition, OEC pilots various offerings and employs its resources to support other DHS plans and programs such as the NECP. Three of these technical assistance offerings are described in detail below. 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, local, and tribal emergency responders, and major intergovernmental and national public safety associations, who provide input on the challenges, needs, and best practices involving emergency communications. The SAFECOM website provides members of the emergency response community and other constituents with information and resources to help them meet their communications and interoperability needs. For more information, see http://www.safecomprogram.gov, or contact SAFECOMGovernance@dhs.gov.

**SAFECOM Guidance on Emergency Communications Grants** provides recommendations to grantees seeking funding for interoperable emergency communications projects, including allowable costs, items to consider when funding emergency communications projects, grants management best practices for emergency communications grants, and information on standards that ensure greater interoperability. The guidance is intended to ensure that Federally-funded investments are compatible and support national goals and objectives for improving interoperability nationwide. For more information see http://www.safecomprogram.gov/grant/Default.aspx or contact the Office of Emergency Communications at oec@hq.dhs.gov.

**The Southwest Border Communications Working Group (SWBCWG)** serves as a forum for Federal, State, local, and tribal agencies in Arizona, California, New Mexico, and Texas to share information on common issues, collaborate on existing and planned activities, and facilitate Federal involvement in multi-agency projects within the Southwest

Border Region. The SWBCWG aims to enhance communications operability and interoperability, effectively use the region's available critical communications infrastructure resources, and ensure that programs continue to meet the stakeholders' needs. For more information on the SWBCWG, e-mail oec@dhs.gov.

**Statewide Communication Interoperability Plans (SCIPs)** are locally-driven, multi-jurisdictional, and multi-disciplinary statewide strategic plans to enhance emergency communications. The SCIP provides strategic direction and alignment for those responsible for interoperable communications at the State, regional, local, and tribal levels. These strategic plans outline and define the current and future vision for communications interoperability within the State or territory. They also align emergency response agencies with the goals, objectives, and initiatives for achieving that vision. SCIPs are living documents that are typically updated on an annual basis, or as frequently as needed. For more information please visit www.dhs.gov/statewide-communication-interoperability-plans.

## **DHS Privacy Office (PRIV)

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

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

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

PRIV is always available to support our state and local partners. Please feel free to contact us via phone: 202-343-1717 and email: privacy@dhs.gov.

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

****Privacy and Cybersecurity**. DHS builds privacy into all its operations. Some areas of DHS operations are particularly sensitive. As part of these high profile activities, DHS created directed public resources to demonstrate the privacy protections it built into the programs – cybersecurity is an example of this directed resource: http://www.dhs.gov/cybersecurity-and-privacy.

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

****Privacy Compliance program, guidance, and templates**. PRIV operates a robust privacy compliance program, using the PIA and other tools to assess and document the integration of rules into the Department's programs and IT systems. To foster public trust through transparency, DHS publishes its PIAs, as well as the templates and guides used to create those PIAs, directly to the public: http://www.dhs.gov/privacy-compliance.

****Policy Establishing the Fair Information Practice Principles as a matter of Department procedure**. DHS believes in a set of privacy principles that guide all DHS strategies, programs, and IT systems. DHS uses these principles as the foundation for new initiatives and privacy impact assessments of existing programs. DHS memorialized these principles as department policy: http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.



*Substantive edits since last update
**New addition to Resource Catalog

****Policy Establishing the Privacy Impact Assessment as a standardized government privacy compliance process**. PRIV uses a structured approach to build privacy protections into specific programs: The Privacy Impact Assessment (PIA). DHS formally established the PIA requirement as a matter of policy: http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-02.pdf.

****Privacy Incident Handling Guidance**. All organizations face the risk of privacy breaches and other incidents. PRIV created a formal approach to preparing for and responding to privacy incidents: http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf.

****Privacy Outreach & Education**. PRIV shares its experience directly with the public and its partners in the public, private, and academic sectors: http://www.dhs.gov/privacy-events.

PRIV issues tailored educational materials to support its government and commercial colleagues, for example: The Handbook for Safeguarding Sensitive Personally Identifiable Information: http://www.dhs.gov/sites/default/files/publications/privacy/Guidance/handbookforsafeguardingsensitivePII_march_2012_webversion.pdf.

## ***Science and Technology (S&T) Directorate***

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

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

All COE work closely with academia, industry, Department components, and first-responders to develop customer-driven research solutions to 'on the ground' challenges as well as provide essential training to the next generation of homeland security experts. The research portfolio is a mix of basic and applied research addressing both short and long-term needs. The COE extended network is also available for rapid response efforts.

Managed through the Office of University Programs, the COE organize leading experts and researchers to conduct multidisciplinary homeland security research and education. Each center is university-led or co-led in collaboration with partners from other institutions, agencies, national laboratories, think tanks and the private sector. For more information, visit http://www.dhs.gov/st-centers-excellence.

**FirstResponder.gov** mission is to provide a portal that enables Federal, state, local, tribal, and territorial first responders to easily access and leverage Federal web services, information on resources, products, standards, testing and evaluation, and best practices, in a collaborative environment. The portal provides first responders with information to develop or deploy technologies that would enhance homeland security. See www.firstresponder.gov.

**First Responder Communities of Practice** is an online network of vetted, active, and retired first responders, emergency response professionals; and Federal, state, local, tribal, and territorial Homeland Security officials sponsored by the DHS S&T's First Responder Technologies program. Registered members of this professional network share information, ideas, and best practices, enabling them to more efficiently and effectively prepare for all hazards. To date, First Responder Communities of Practice has more than 5,000 active members and nearly 200 active communities based on diverse interests and disciplines. See www.firstresponder.gov or https://communities.firstresponder.gov.



*Substantive edits since last update
**New addition to Resource Catalog

*The **First Responders Group** is S&T's component that works directly with first responder organizations to identify and prioritize gaps in capabilities, establish operational requirements and standards, and develop and commercialize solutions. Projects in the First Responders Group three strategic thrust areas – increasing responder safety and effectiveness, enabling communications, and providing a common operating picture – result directly from close collaboration with the end users. Reflecting our focus on transition, we have worked to ensure that technologies developed in coordination with S&T are available to first responder communities nationwide; S&T's technologies are included in the Federal Emergency Management Agency's Authorized Equipment List that public safety agencies are authorized to purchase from with their Federal grant dollars.

The First Responders Group is also working to develop a virtual environment that every jurisdiction within the country can access, train within, and modify to meet their individual needs. S&T is leveraging investments and technological advances made by the military, specifically the U.S. Army's prototype virtual environment called Enhanced Dynamic Geo-Social Environment (EDGE) Virtual Training. S&T is using EDGE to develop a series of realistic, first responder-identified scenarios. The scenarios will have varying levels of difficulty and will require users to successfully employ tactics, techniques, and procedures to respond. The tool also has a strategic component requiring responders to establish Unified Command to manage complex cross discipline events. S&T worked with first responders to identify critical incidents and chose an active shooter for the first scenario. S&T worked with the U.S. Army to create a 3-D environment for the scenario, as well as accurate avatars, equipment, and simulations of individuals and crowds. S&T is currently piloting this scenario with emergency response agencies in Sacramento, California, and collecting feed-back to further refine the scenario. Eventually, S&T plans to incorporate this scenario, as well as others, into a customizable, multi-player online game that is interoperable with multiple user interfaces (e.g., joy stick, keyboard, gaming console).

****The First Responder Resource Group (FRRG)** serves as a mechanism for continuous dialogue and the coordination of research, development and delivery of technology solutions to first responders and the emergency preparedness and response community at the local, state, tribal, territorial, and federal levels. More than 120 responders from around the country are engaged throughout S&T's established solution development process to identify, validate, and facilitate the fulfillment of first responder needs through the use of existing and emerging technologies, knowledge products, and standards. The group meets annually in person and virtually throughout the year.

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

## ***United States Secret Service (Secret Service)***

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

**Computer Emergency Response Team (CERT) at Carnegie Mellon**. In August 2000, the Secret Service and the Software Engineering Institute, a Federally-funded research and



*Substantive edits since last update
**New addition to Resource Catalog
2/24/14

development center located at Carnegie Mellon University, instituted the Secret Service Computer Emergency Response (CERT) liaison program. This program positions the Secret Service to meet emerging cyber security threats as part of the agency's investigative and protective missions. The agents assigned to the CERT liaison program lead Secret Service-sponsored research and development as well as direct technical support for investigative and protective operations. The agents assigned to the CERT liaison program work closely with the Software Engineering Institute and Carnegie Mellon University to identify and implement advanced technology in support of the full spectrum of Secret Service operations. CERT does distribute forensic tools developed at the university to state and local law enforcement agencies. For more information, 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 digital equipment and information obtained through private partnerships to monitor developing technologies and trends in the financial payments industry. This information is used to enhance the Secret Service's capabilities to prevent and mitigate attacks against the financial and critical infrastructures. CIS has developed an operational investigative unit, which targets, pursues, and arrests international cyber criminals involved in cyber intrusions, identity theft, credit card fraud, bank fraud, and other computer-related crimes. CIS provides crucial information and coordination to facilitate the successful dismantling of international criminal organizations. 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's eInformation Network is available – for free – to authorized law enforcement officers, financial institution investigators, academic partners, and commercial partners of the Secret Service. The site contains two tools: the eLibrary, a unique collection of resource databases which allows authorized users from throughout the law enforcement community to obtain information on a range of sensitive topics including counterfeit corporate checks, credit card issuing bank information, and recovered skimming devices; and the U.S. Dollars Counterfeit Note Search, a site that provides the user with the ability to conduct a search of the Secret Service counterfeit note database. For more information, 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. 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 33 Secret Service ECTFs, to include London, England and Rome, Italy. Membership in the Secret Service ECTFs include approximately 300 academic partners; over 2,200 international, Federal, state, and local law enforcement partners; and over 3,000 private sector partners. Through the ECTFs, local and state law enforcement officers may request investigative assistance from the Secret Service's Mobile Wireless Investigations teams. There are currently 22 MWI teams throughout the United States. For more information, 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 U.S. financial system from the abuses of criminal activities to include terrorist financing, money laundering, and other illicit activity. For more information, please contact your local Secret Service Field Office at 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.

**Mobile Device Forensic Facility**. The Mobile Device Forensic Facility in Tulsa, OK was created in 2008 to meet the challenges associated with the forensic extraction of data from mobile devices. The Secret Service established a partnership with the University of Tulsa, Digital Forensic Laboratory Center of Information Security to create and co-locate the Mobile Device Forensic Facility at the University. The facility provides training and conducts forensic examinations and research on mobile devices. The ongoing research into these new devices, operating systems and mobile device technologies provides valuable tools in the Secret Service's fight against cybercrime. 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.

**National Center for Missing and Exploited Children**. The Secret Service supports the National Center for Missing and Exploited Children and local law enforcement with its expertise in forensic analysis to include crime scene, handwriting, document authentication, ink analysis, fingerprints and photography, graphic design, video productions, audio/image enhancement and speaker recognition services. Specialized polygraph and crime scene services are evaluated upon request. For more information, 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 12 courses: Basic Investigation of Computer and Electronic Crimes Program, Basic Computer Evidence Recovery Training, Advanced Forensics Training, Basic Network Investigation Training, Network Intrusion Response Program, Basic Mobile Device Investigations, Mobile Device Examiner, Advance Mobile Device Examiner, Online Social Networking, Computer Forensics in Court – Prosecutors, Computer Forensics in Court – Judges, Mobile Devices in Court – Prosecutors. NCFI provides funding for all travel expenses, hotel and per diem for state and local law enforcement officers. Additionally, all NCFI graduates receive hardware, software and licenses necessary to conduct forensic computer and network intrusion examinations. For more information, see www.ncfi.usss.gov.

## Transportation Security Administration (TSA)

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

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

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

227-5150 or email ISTEP@dhs.gov.

- Managed by the I-STEP, the **Exercise Information System (EXIS)** is the only exercise tool specifically tailored to the transportation sector. EXIS takes a step-by-step approach as it guides users though exercise planning. First it directs users to identify the exercise planning schedule and sector focus; next it enables users to select specific objectives and scenario elements; and finally, it allows users to plan evaluation criteria, share best practices and lessons-learned, and create post-exercise reports. EXIS communities facilitate information sharing among users. Users can create private communities and sub-communities to design operator-specific exercises and to delegate tasks to other planning team members. EXIS is provided at no cost by the TSA as an integral part of I-STEP. To become an EXIS member, visit http://exis.tsa.dhs.gov. For further information please contact EXIS@dhs.gov.

**Joint Vulnerability Assessment (JVA) Training**. The Security Assessments Section (SAS), under the Office of Law Enforcement/Federal Air Marshal Service, Security Services and Assessments Division conducts JVAs in partnership with the FBI for the purpose of assessing current and potential threats to commercial air transportation facilities within the United Sates. The assessment process is a direct result of the increasing threat to aviation, a threat which prompted Congress to pass Section 310 of the Federal Aviation Reauthorization Act of 1996, requiring the Federal Aviation Administration (FAA) and the FBI to conduct joint threat and vulnerability assessments of security at U.S. airports. In response to this mandate, during Fiscal Years (FY) 1999, 2000, and 2001, FAA and FBI prepared three-part assessments addressing the vulnerability, criminal activity, and terrorist threat at selected airports nationwide. In FY 2002, TSA took on the responsibility of conducting assessments from the FAA pursuant to the Aviation and Transportation Security Act. When SAS 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. SAS 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 presence and support of passenger screening activities at U.S. commercial airports.

**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 SAS, under the Office of Law Enforcement/Federal Air Marshal Service, Security Services and Assessments Division, 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. SAS also provides oversight and guidance on the development and implementation of MANPADS mitigation plans at the commercial airports.

SAS provides MANPADS awareness training to local law enforcement and other first responders. TSA also provides MANPADS pocket identification cards and posters to law enforcement and first responders to assist in the identification of MANPADS and their components.
For further information please email: OLEFAMSOSA@dhs.gov.

**National Explosives Detection Canine Team Program (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 Law Enforcement Officer (LEO) Flying Armed Training Program**. The TSA Office of Training and Workforce Engagement, Law Enforcement and Industry Training Division is responsible for oversight of the TSA LEO Flying Armed Training Program, which is *mandatory* for all law enforcement officers flying armed under the Code of Federal Regulation 1544.219, Carriage of Accessible Weapons. The LEO Flying Armed training is a 1.5 to 2 hour block of instruction that is comprised of a structured lesson plan, slide presentation, FAQs, NLETS procedures, and applicable codes of Federal regulation. This material is provided to Federal, state, local, territorial, tribal, and approved railroad law enforcement agencies and departments to properly instruct their officers on the subject of flying on board commercial aircraft while armed. The training includes protocols in the handling of prohibited items, prisoner transport, and dealing with an act of criminal violence aboard an aircraft. The program training material may be obtained by emailing the TSA Office of Training and Workforce Engagement, Law Enforcement and Industry Training Division, at LEOFA@dhs.gov.
To request this training material you must:

- Be a full-time law enforcement officer meeting the instructor qualification standards of the agency, academy, or department in which you are employed;
- Send the request from a governmental email address; and
- Include the following information in the body of the email: (1) Your name and contact information; (2) Your department's name and address; and (3) Your supervisor's name and contact information.

If you are not a qualified instructor, please request a member of your training staff to contact us by email. For time

sensitive training requests, please call (855) 359-5367 between the core business hours of 9:00 am to 5:00 pm EST.

The TSA Call Center (TCC) is responsible for fielding incident reports from the public. TSA's Inspections and Investigations Division (IID) is responsible for conducting criminal and administrative investigations of employees who are alleged to have committed misconduct, including identifying and investigating potential worker's compensation fraud by TSA employees.

If a person suspects that a TSA employee is engaging in misconduct or fraud, they are asked to e-mail TSAInspectionHotline@dhs.gov. They are asked to provide the name of the employee suspected for alleged misconduct and an explanation of the issue, including date(s) and time(s). They are also asked to provide their name and contact information for appropriate follow-up. Employees should provide their name even if they choose to remain anonymous throughout the process.

The public may also report security-related incidents to TCC, and may request follow up information on the status of those reports through TCC.

## ACRONYMS

| | |
|---|---|
| ACAMS | Automated Critical Asset Management System |
| AMOC | Air and Marine Operations Center |
| ANSI | American National Standard Institute |
| AUXCOMM | Auxiliary Communications |
| BCOP | Biosurveillance Common Operating Picture |
| BCSC | National Bulk Cash Smuggling Center |
| BEST | Border Enforcement Security Task Force |
| BMAP | Bomb-making Material Awareness Program |
| BSC | Biometric Support Center |
| C3 | Cyber Crime Center |
| CBP | U.S. Customs and Border Protection |
| CDF | Capability Development Framework |
| CDP | FEMA Center for Domestic Preparedness |
| CFATS | Chemical Facility Anti-Terrorism Standards |
| CGMIX | USCG Maritime Information eXchange |
| CI | Critical Infrastructure |
| CIS | Cyber Intelligence Center |
| CIFW | Counterintelligence Fundamental Workshop |
| COE | Centers of Excellence |
| COI | Community(ies) of Interest |
| COML | Communications Unit Leader |
| CRADA | Cooperative Research and Development Agreement |
| CRCL | Office for Civil Rights and Civil Liberties |
| CRR | Cyber Resiliency Review |
| CSEP | Cybersecurity Evaluation Program |
| CVE | Countering Violent Extremism |
| DARTTS | Data Analysis & Research for Trade Transparency Systems |
| DBFTF | Document and Benefit Fraud Task Force |
| DHS | Department of Homeland Security |
| DHS-SPS | DHS Single Point of Service |
| DNDO | Domestic Nuclear Detention Office |
| DOE | Department of Energy |
| DOJ | Department of Justice |
| DSF | Deployable Special Forces |
| ECSAP | Electronic Crimes Special Agent Program |
| ECTF | Electronic Crimes Task Force |
| EDCT | Explosive Detection Canine Team |
| EDD | Explosive Detector Dog |
| EDGE | Enhanced Dynamic Geo-Social Environment |
| EEO | Equal Employment Opportunity |
| EMI | Emergency Management Institute |
| EOC | Emergency Operations Center |
| ERO | ICE Enforcement and Removal Operations |
| ESS | Emergency Sector Services |
| ESS-CRA | Emergency Sector Services-Cyber Risk Assessment |
| ESTA | Electronic System for Travel Authorization |
| EXIS | Exercise Information System |
| FBI | Federal Bureau of Investigation |
| FCTC | Financial Crimes Task Force |
| FDNS | Fraud Detection and National Security |
| FAA | Federal Aviation Administration |
| FEMA | Federal Emergency Management Agency |
| FinCEN | Financial Crimes Enforcement Network |
| FiRST | First Responder Support Tool |
| FLETC | Federal Law Enforcement Training Centers |
| FPS | Federal Protective Services |
| FRRG | First Responder Resource Group |
| HSDN | Homeland Security Data Network |
| HSI | ICE Homeland Security Investigations |
| HSI-FL | HSI Forensics Laboratory |
| HSIN | Homeland Security Information Network |
| I&A | Office of Intelligence and Analysis |
| IED | Improvised Explosive Device |
| IEEE | Institute of Electrical and Electronics Engineers |
| ICE | U.S. Immigration and Customs Enforcement |
| ICS-CERT | Industrial Control Systems Cyber Emergency Response Team |
| ICTAP | OEC Interoperable Communications Technical Assistance Program |
| IMAGE | ICE Mutual Agreement between Government and Employers |
| INTERPOL | International Criminal Police Organizaiton |
| IOC-2 | International Organized Crime Intelligence and Operations Center |
| IP | Intellectual Property |
| IPAWS | Integrated Public Alert and Warning System |
| IPR Center | National Intellectual Property Rights Coordination Center |
| IPTET | Intellectual Property Theft Enforcement Team |
| ITA | Intelligence Training Academy |
| JAC | Joint Analysis Center |
| JACCIS | JAC Collaborative Information System |
| JVA | Joint Vulnerability Assessment |
| LEO | Law Enforcement Officer |
| MANPADS | Man-Portable Air Defense Systems |
| LEISI | Law Enforcement Information Sharing Initiative |
| LMS | FLETC Learning Management System |
| MCV | Mobile Command Vehicle |
| MDDP | Mobile Detection Deployment Program |
| MDDU | Mobile Detection Deployment Unit |
| MJIEDSP | Multi-Jurisdictional Improvised Explosive Device Security Planning |
| MS-ISAC | Multi-State Information Sharing Center |
| NBIC | National Biosurveillance Integration Center |
| NCC | National Coordination Center |
| NCCIC | National Cybersecurity and Communications Integration Center |
| NCFI | National Computer Forensics Institute |
| NCSAM | National Cybersecurity Awareness Month |
| NECP | National Emergency Communications Plan |
| NEDCTP | National Explosives Detection Canine Team Program |
| NGO | Nongovernmental Organization |
| NIFOG | National Interoperability Field Operations Guide |
| NIMS | National Incident Management System |
| NIMS ICS | NIMS Incident Command System |
| NIPP | National Infrastructure Protection Plan |
| NNSA | National Nuclear Security Administration |
| NPPD | National Protection and Program Directorate |
| NTAS | National Terrorism Advisory System |

| | |
|---|---|
| NTED | National Training and Education Division |
| OBMI | Office of Biometric Identity Management |
| OBP | Office of Bombing Prevention |
| OCSTF | Operation Community Shield Task Forces |
| ODLS | Online Detainee Locator System |
| OEC | Office of Emergency Communications |
| OHA | Office of Health Affairs |
| OIG | Office of Inspector General |
| OSLLE | Office for State and Local Law Enforcement |
| OSLTC | ICE Office of State, Local, and Tribal Coordination |
| PED | UCSIS Public Engagement Division |
| PIA | Privacy Impact Assessment |
| PII | Personally Identifiable Information |
| PRIV | DHS Office of Privacy |
| PRND | Preventative Radiological/Nuclear Detection |
| RAP | Radiological Assistance Program |
| RAPP | Regional Analytic Advisor Plan |
| RFI | Request for Information |
| RKB | Response Knowledge Base |
| RISS | Regional Information Sharing System |
| RND | Radiological and Nuclear Detection |
| S&T | Science and Technology Directorate |
| SAS | Security Assessment Section |
| SAVER | System Assessment and Validation for Emergency Responders |
| SEVP | Student Exchange Visitor Program |
| SLRTT | FLETC Office of State, Local, Tribal, and Territorial Training |
| SLT | CBP State, Local, Tribal, Liaison |
| SLTT | State, local, tribal, and territorial |
| SSI | Sensitive Security Information |
| STC | Security the Cities |
| US-CERT | U.S. Computer Emergency Readiness Team |
| USCG | U.S. Coast Guard |
| USCIS | U.S. Citizenship and Immigration Services |
| TCL | Target Capability List |
| TCC | TSA Call Center |
| TRIPwire | Technical Resource for Incident Prevention |
| TSA | Transportation Security Administration |
| TTU | Trade Transparency Unit |
| UASI | Urban Area Security Initiative |
| VAP | Victims Assistance Program |
| VAWA | Violence Against Women Act |
| VBIED | Vehicle-borne Improvised Explosive Device |
| VWP | Visa Waiver Program |

**APPENDIX**

**#**

287(g) – 23

**A**

Active Shooter – 30, 31, 39, 40, 45
America's Waterways Watch – 14
Arab and Muslim American Cultural Awareness –12, 13
Aviation Security – 16, 48, 49

**B**

Bank Fraud – 46
Biometrics – 31
Biosurveillance – 23
Blue Campaign to Fight Human Trafficking – 6
Border Community Liaison Program (CBP) – 15
Border Enforcement Security Task Force – 23
Bulk Cash Smuggling – 26

**C**

Carrier Liaison Program (CBP) – 15
Centers of Excellence - 44
**Citizenship and Immigration Services – 7**
**Citizenship and Immigration Services Ombudsman Office – 10**
**Civil Rights and Civil Liberties (Office of) – 9**
**Coast Guard – 14**
Continuity of Operations – 21
Counterfeiting – 26, 46
Countering Violent Extremism – 11
Counterintelligence – 29
Credit Card Fraud – 46
Critical Infrastructure – 34, 35, 36, 37, 38, 38, 40, 41
**Customs and Border Protection – 15**
Cyber Crime – 24, 47
Cybersecurity – 24, 34, 35, 36, 37, 43, 47

**D**

Daily Intelligence Reports (Open Source) – 29
Department of Motor Vehicle Fraud – 25
Detainee Locator (Online) – 27
**Domestic Nuclear Detection Office – 16**
Drug Trafficking – 16, 28

**E**

Electronic Crimes – 46, 47, 48
Electronic System for Travel Authorization – 15
Emergency Communications – 36, 41, 42, 43
Emergency Management Training – 21
Emergency Operations Center – 20
Employment Eligibility Verification – 8
Enforcement and Removal Operations – 23, 29
English as a Second Language – 10, 12
Equal Employment Opportunity – 11
Explosives – 31, 32, 33, 37, 50
Explosive Detection Dogs – 37, 50
E-Verify – 7, 8, 9, 11

**F**

**Federal Emergency Management Agency – 20**
**Federal Law Enforcement Training Centers – 22**
Financial Crimes – 47
FirstResponder.gov – 44, 45
Flying-Armed Training Program – 50
Forced Labor – 24
Forensics (Computers) – 48
Forensics (Laboratory) – 24, 25
Forensics (Mobile Devices) – 47
Fusion Centers – 12, 20, 29, 30

**G**

Gangs – 26
Grants – 21

**H**

**Health Affairs (Office of) – 22**
Homeland Security Information Network (HSIN) – 6
Homeland Security Investigations – 23
Human Rights and Vulnerable Populations – 12, 25
Human Trafficking – 6, 9, 16, 27, 29

**I**

I-9 (Form) – 8
Identity Theft – 46
If You See Something, Say Something™ – 6
Illicit Trafficking – 16
**Immigration and Customs Enforcement – 23**
Immigration Document and Benefit Fraud – 24
Immigration Enforcement (Campus) – 27
Immigration Services – 7
Improvised Explosive Device – 31, 32, 33, 34
Information Technology – 36
Infrastructure Protection – 38, 39, 40
Inspector General – 6
Intellectual Property Rights – 15, 26
**Intelligence and Analysis (Office of)** – 29
Intermodal Security – 48
International Non-Custodial Parental Child Abduction – 16
International Travel and Trade – 16

**K**

K-9 Training – 37, 50

**L**

Language Identification Pocket Guide – 12
Law Enforcement Information Sharing Initiative - 25
Limited English Proficiency – 10, 12, 13

**M**

Man-Portable Air Defense Systems (MANPADS) – 49
Maritime Navigation – 14
Missing and Exploited Children – 48
Missing or Late International Travelers – 16
Mobile Command Vehicles – 38
Money Laundering – 28, 47
Multi-State Information Sharing and Analysis Center – 36

**N**

National Incident Management System – 21, 41
**National Protection and Program Directorate – 30**
National Terrorism Advisory System – 6
Naturalization – 7
Nuclear Detection – 16, 17, 18, 19, 20

**O**

Organized Crime – 47

**P**

Pipelines (Safeguarding) – 48
Port of Entry – 16
Preparedness (Non-Disaster) Grants – 21
Privacy – 43, 44
Prosecutions (Toolkit) – 28

**R**

Racial Profiling – 12
Radiological Detection – 16, 17, 18, 19, 20
Responder Knowledge Base – 17, 22
Retail Security – 39

**S**

S Visa Program – 8
**Science and Technology Directorate (S&T) – 44**
**Secret Service – 45**
Secure Communities – 13, 27
Self-Check (*see* E-Verify) – 7, 9
Sensitive Security Information (Safeguarding) – 50
Shadow Wolves – 27
Student and Exchange Visitor Program – 27, 28
Suspicious Aircraft or Boats – 16

**T**

Tip Line (CBP) – 16
Tip Line (HSI) – 25
Title 19 Cross–Designation – 28
Title VI – 10
Training – 6, 9, 11, 12, 13, 15, 19, 20, 21, 22, 25, 26, 27, 28, 29, 30, 31, 32, 34, 36, 38, 39, 40, 44, 45, 47, 48, 49, 50
**Transportation Security Administration – 48**
Tribal Law Enforcement – 27
TRIP*wire* – 33, 34
T Visa – 9

**U**

USCG Sector Command Centers – 15
USCIS Applications – 10
USCIS Case Assistance – 10
USCIS Petitions – 10
U Visa – 7, 9

**V**

Vehicle-borne Improvised Nuclear Device – 32
Victim Assistance – 29
Violence Against Women Act – 9
Visa Waiver Program – 15, 16
Visas for Victims of Human Trafficking and Other Serious Crimes – 9

**W**

Workplace Security – 40