Department-wide Resources

Civil Rights, Civil Liberties, and Privacy

Blue Campaign Toolkit provides private sector stakeholders with a compiled list of training, resources, and actions you can take to combat human trafficking and raise awareness. It also provides links to anti-human trafficking resources available from other Federal Departments and Agencies. The Toolkit is available at http://www.dhs.gov/files/programs/gc_1281551408757.shtm.

Blue Campaign to Combat Human Trafficking is the Department of Homeland Security's first-of-its-kind initiative to coordinate and enhance the Department's anti-human trafficking efforts, led by a cross-component steering committee, which is chaired by the Senior Counselor to the Secretary. ICE is the primary agency within DHS that investigates human trafficking, and it runs a 24 hour hotline 1-866-DHS-2ICE (1-866-347-2423), for the public to report suspicious activity. The public can also call the National Human Trafficking Resource Center Hotline (888-3737-888) to reach a non-governmental organization. Informational human trafficking materials are available in a variety of languages, and include public service announcements, brochures, indicator cards, shoe cards, and tear cards. For more information, see http://www.dhs.gov/humantrafficking.

The Office for Civil Rights and Civil Liberties (CRCL) Annual Reports to Congress Under 6 U.S.C. § 345 and 42 U.S.C. § 2000ee-1, CRCL is required to report annually to Congress about the activities of the Office. For more information, or to view the reports, please visit www.dhs.gov/crcl.

Community Roundtables The DHS Office for Civil Rights and Civil Liberties (CRCL) leads, or plays a significant role, in regular roundtable meetings among community leaders and federal, state, and local government officials. These roundtables bring together American Arab, Muslim, South Asian, Middle Eastern, and Sikh communities with government representatives; other roundtables include immigrant communities and those with frequent DHS contacts. CRCL also conducts roundtables with young leaders of diverse communities. For more information please contact CRCLOutreach@dhs.gov.

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 Monthly Newsletter is distributed monthly to inform 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, posted on the CRCL website (www.dhs.gov/crcl), and made available to community groups for redistribution. Please contact CRCLOutreach@dhs.gov for more information.

Environmental Justice Annual Implementation Report Environmental justice (EJ) describes the commitment of the government to avoid placing disproportionately high and adverse burdens on the human health and environment of minority populations or low-income populations through its policies, programs, or activities. Executive Order 12898, *Federal Actions to Address Environmental Justice in Minority Populations and Low Income Populations* (E.O. 12898), was established in 1994 and directs federal agencies to make achieving environmental justice part of their mission. As part of our responsibilities in this E.O., DHS recently published an Environmental Justice Annual Implementation Report. For more information, or to view the report, see http://www.dhs.gov/xlibrary/assets/mgmt/dhs-fy2011-ej-ann-rpt.pdf.

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.

Forced Labor Resources The ICE Homeland Security Investigations (HSI) Office of International Affairs investigates allegations of forced labor in violation of the Tariff Act of 1930 (Title 19 USC §1307). To request more information or a copy of the A Forced Child Labor Advisory booklet and brochure, please contact: ice.forcedlabor@ice.dhs.gov. When contacting ICE to report instances of forced labor, please provide as much detailed information and supporting documentation as possible, including the following: a full statement of the reasons for the belief that the product was produced by forced labor and that it may be or has been imported into the United States; a detailed description of the product; all pertinent facts known regarding the production of the product abroad. For the location of ICE foreign offices, please visit the ICE web site at http://www.ice.gov, click About Us, click International Affairs and select your country. ICE maintains a 24/7 hotline at (866) DHS-2-ICE (866-347-2423).

Guide to Implementing Privacy informs the public about how the DHS Privacy Office implements privacy at DHS. The guide provides an overview of the DHS Privacy Office's functions and transparency in day-to-day operations. For more information please visit http://www.dhs.gov/xabout/structure/editorial_0338.shtm.

Guidance to Federal Financial Assistance Recipients Regarding Title VI Prohibition Against National Origin Discrimination Affecting Limited English Proficient Persons On April 18, 2011 DHS, in pursuance of Executive Order 13166 "*Improving Access to Services for Persons with Limited English Proficiency*" published this guidance to help those with limited English proficiency. For more information, see http://www.dhs.gov/xabout/laws/gc_1277242893223.shtm.

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 CRCLOutreach@dhs.gov.

Human Rights Violators and War Crimes Center protects the public by targeting war criminals and those who violate human rights, including violators living both domestically and abroad. ICE investigators, intelligence analysts, and attorneys work with governmental and non-governmental agencies to accept tips and information from those who report suspected war criminals and human rights violators. Individuals seeking to report these abuses of human rights may contact the center at HRV.ICE@dhs.gov.

If You Have the Right to Work, Don't Let Anyone Take it Away Poster is a poster with Department of Justice information regarding discrimination in the workplace. See http://www.uscis.gov/files/nativedocuments/e-verify-swa-right-to-work.pdf.

Introduction to Arab American and Muslim American Cultures is an hour-long training DVD that provides insights from four national and international experts. 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 crcl@dhs.gov or visit www.dhs.gov/crcl.

Language Access CRCL provides resources, guidance and technical assistance to recipients of financial assistance from DHS to help ensure meaningful access to persons who are Limited English Proficient (LEP) as required by Title VI of the Civil Rights Act of 1964. CRCL is a member of the Federal Interagency Working Group on LEP, which hosts www.LEP.gov. Additionally, on February 28, 2011 DHS released it's first-ever Department plan for providing meaningful access to homeland security programs to people with limited English proficiency. For more information, see http://www.dhs.gov/files/publications/dhs-language-access-plan.shtm or contact crcl@dhs.gov.

Minority Serving Institutions (MSIs) Programs include the Scientific Leadership Award (SLA) grant program, and the Summer Research Team program. Both improve the capabilities of MSIs to conduct research, education, and training in areas critical to homeland security and to develop a new generation of scientists capable of advancing homeland security goals. The SLA program provides three to five years of institutional support for students and early career faculty. The Summer Research Team programs provide support for a ten week collaborative research experience between recipient MSIs and the Centers of Excellence. For more information, please visit: Historical Funding Opportunity Announcements (CDG and SLA) http://grants.gov/; DHS Scholars Program http://www.orau.gov/dhsed/; Summer Research Team Program http://www.orau.gov/dhsfaculty/. For more general information, please contact universityprograms@dhs.gov.

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

No te Engañes (Don't be Fooled) is the Customs and Border Protection (CBP) outreach campaign to raise awareness about human trafficking among potential migrants. For more information, please visit http://www.cbp.gov/xp/cgov/border_security/human_trafficking/ or contact Laurel Smith at laurel.smith@dhs.gov or 202-344-1582.

Posters on Common Muslim American Head Coverings, Common Sikh American Head Coverings, and the Sikh Kirpan These training posters provide guidance to Department personnel on ways in which to screen, if needed, Muslim or Sikh individuals wearing various types of religious head coverings and Sikh individuals carrying a Kirpan (ceremonial religious dagger). To obtain the posters, please visit www.dhs.gov/crcl or contact crcl@dhs.gov.

Privacy Impact Assessments (PIAs) are decision-making tools used to identify and mitigate privacy risks at the beginning of and throughout the development life cycle of a program or system. They help the public understand what personally identifiable information (PII) the Department is collecting, why it is being collected, and how it will be used, shared, accessed, and stored. All PIAs issued by DHS may be found here: http://www.dhs.gov/files/publications/editorial_0511.shtm.

DHS Privacy Office sustains privacy protections and the transparency of government operations while supporting the DHS mission. The DHS Privacy Office ensures DHS programs and operations comply with federal privacy laws and policies. Members of the public can contact the Privacy Office with concerns or complaints regarding their privacy. For more information, visit www.dhs.gov/privacy or contact privacy@dhs.gov, (202) 235-0780.

DHS Privacy Office Disclosure and Transparency Private sector organizations can use the Freedom of Information Act (FOIA) to get specific information from Federal agencies. To view the process for submitting a FOIA request, or to see a library of past requests, please visit http://www.dhs.gov/xfoia/editorial_0579.shtm.

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

Resources for Victims of Human Trafficking and Other Crimes USCIS has a variety of resources for victims of human trafficking including Immigration Remedies for Trafficking Victims, Immigration Options for Victims of Crimes (in Spanish, Russian, and English), and a 'How Do I' Guide for Nonimmigrants. To access these and other resources, please visit the "Resources" section of www.uscis.gov and find the link on the left side.

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 headquarters personnel and Victim Assistance Coordinators in the field also provide training and technical assistance to special agents, law enforcement partners, and other agencies. Full-time Forensic Interview Specialists are also available to conduct developmentally appropriate, legally defensible, and victim-sensitive interviews in HSI cases involving child, adolescent, or special needs victims. 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.

Economic Analysis

Computable General Equilibrium (CGE) Economic Analysis Model and Expanded Framework is a state of the art methodology for performing economic consequence analysis. For more information, see http://create.usc.edu/research/Measuring Economic Resilience to Terrorism.pdf.

DHS Center of Excellence: National Center for Risk and Economic Analysis of Terrorism Events (CREATE) develops tools to evaluate the risks, costs, and consequences of terrorism, and guides economically viable investments in countermeasures. Resources include: ARMOR (Assistant for Randomized Monitoring over Routes), IRIS (Intelligent Randomization in International Scheduling), and PROTECT (Port Resilience Operational/Tactical Enforcement to Counter Terrorism). ARMOR is a software program that randomizes patrols, inspections, schedules, plans or actions carried out by security agencies. GUARDS (Game Theoretic Security Allocation on a National Scale) is another resource developed by the Center of Excellence. This software application assists in resource application tasks for airport protection. GUARDS deals with three key issues: (i) reasoning about hundreds of heterogeneous security activities; (ii) reasoning over diverse potential threats; (iii) developing a system designed for hundreds of end-users. PROTECT allows security forces to randomize patrols, searches, and check-points based on critical assets and intelligence. For more information, see http://teamcore.usc.edu/security/.

National Interstate Economic Model (NIEMO) is an operational multi-regional input-output economic impact model of 50 states and DC that develops economic analysis results for 47 economic sectors. For more information, see http://create.usc.edu/research/50822.pdf.

Outreach and Engagement

Building Resilience through Public-Private Partnerships Conference Although online resources are valuable in their broad accessibility, sometimes face-to-face opportunities are the best way to fully engage people and encourage a productive exchange of ideas. The national conference on "Building Resilience through Public Private Partnerships" was held in August 2011, and a second conference is planned for July 23-24, 2012 in Colorado Springs, Colorado. Combined in-person and virtual participation for the 2011 event reached close to 1,000 people nationwide. The conference was developed in collaboration with DHS HQ and USNORTHCOM and was co-hosted at the U.S. Chamber of Commerce and the American Red Cross Headquarters. The conference after action report is available on www.fema.gov/privatesector. USNORTHCOM is leading planning for the 2012 conference. Please contact ncc.icgps.omb@northcom.mil for more information.

CBP Industry Partnership and Outreach Program serves as CBP's primary interface to industry for education and information on procurement opportunities, and it's Small Business Program. The program is responsible for processing unsolicited proposals and includes in its organizational structure, CBP's procurement ombudsman. Officially servicing as CBP's "Task and Delivery Order Ombudsman," the program director addresses vendors' concerns or complaints, relating to task or delivery order award procedures. All inquiries are handled in an impartial (and upon request, confidential) manner. Vendors seeking information on how to do business with CBP should go to http://www.cbp.gov/xp/cgov/toolbox/contacts/contracting/ or send an email to CBP's Industry Communication Liaison at the following email address: robert.namejko@cbp.gov. Vendors seeking assistance of the Task Order Ombudsman should send an email to francine.harris@dhs.gov.

Critical Manufacturing Working Groups Critical Manufacturing SCC and GCC members have the opportunity to participate in the CM Information Sharing Working Group and the CM Cyber Security Working Group. The Working Groups provide a platform for industry and government to discuss topics of interest and exchange best practices. Meetings occur on a monthly basis and are posted on the CM HSIN site. For more information, see http://www.dhs.gov/files/committees/gc_1277402017258.shtm or email hsin.outreach@dhs.gov.

Cross-Sector Supply Chain Working Group (CSSCWG) In December 2010, the Critical Manufacturing Sector co-sponsored the development of the Cross-Sector Supply Chain Working Group (CSSCWG), bringing together the 18 Critical Infrastructure Sectors to explore security issues surrounding the supply chain. One major goal of the working group is to review and share both the best practices and known gaps, in order to streamline the various supply chain efforts. For more information see http://www.dhs.gov/files/committees/gc_1277402017258.shtm or email NICC@dhs.gov.

The **DHS Operations Special Events Program (SEP)** is designed to address special events that are not designated as National Special Security Events (NSSEs). The SEP provides a framework through which federal, state, local, and territorial entities can identify special events occurring within their jurisdictions; request federal support; and, after evaluation and assessment, receive appropriate federal support. The SEP also supports the United States Secret Service in its execution of NSSEs. A primary responsibility of the SEP is to support the Federal Coordinator (FC) (when designated by the Secretary of DHS for select events). The SEP provides the FC with a scalable Special Events Support Cell that deploys to the special event, providing subject matter expertise, situation reporting, and interagency/inter-government liaison. The SEP mission is to assure that information regarding special events is shared across the federal government and that resource needs are communicated across the agencies with responsibility for special event response. The SEP achieves this mission through collaboration with the interagency SEWG. For more information, please contact OPS-SEWG@hq.dhs.gov.

DHS Center for Faith-based & Neighborhood Partnerships (CFBNP) builds, sustains, and improves effective partnerships between government sectors and faith-based and community organizations. Located within FEMA, CFBNP is a vital communication link and engagement partner for faith-based and community organizations across the entire Department of Homeland Security. Visit www.dhs.gov/fbci. For more information or to sign up to receive Information Updates, e-mail Infofbci@dhs.gov.

DHS for a Day This program was launched in 2010 to educate and engage the Department's private sector partners on the Homeland Security Enterprise. As of May 2012, the DHS Private Sector Office had coordinated nine events across the country focusing on issues ranging from supply chain security to emergency operations. For more information, see the Blog @ DHS or email DHSforaDay@dhs.gov.

DHS Industry Liaisons: These component Industry Liaisons provide communication with industry. Industry is encouraged to contact representatives when there are questions about conducting business with DHS. Find contact information at http://www.dhs.gov/xopnbiz/opportunities/industry-communication-liaisons.shtm

DHS Loaned Executive Program Come work for DHS! The Loaned Executive Program provides an excellent opportunity (unpaid) for private sector subject matter experts from across sectors and industries to serve in a unique capacity on temporary rotation or sabbatical at DHS. If you or your company are interested in becoming more involved, please e-mail loanedexecutive@dhs.gov.

DHS Loaned Professor Program (via the Intergovernmental Personnel Act Mobility Program) Spend your sabbatical at DHS! Contribute to our nation's security and gain in depth experience on homeland security issues ranging from cybersecurity to trade facilitation. For more information, please email loanedexecutive@dhs.gov.

The **DHS Private Sector Office (PSO)** serves as the primary advisor to the Secretary on all homeland security issues that impact the private sector, defined as businesses, academic institutions, trade associations, not-for-profits, and other non-governmental-organizations. PSO also works to create and foster strategic communications with the private sector and to interface with other relevant federal agencies to help create a more secure nation. For more information on PSO, see http://www.www.dhs.gov/privatesector or call 202-282-8484.

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

FEMA Private Sector E-alerts are periodic e-alerts providing timely information on topics of interest to private sector entities. To sign up for these and other alerts visit http://www.fema.gov/help/getemail.shtm.

FEMA Small Business Industry Liaison Program provides information on doing business with FEMA, specifically with regard to small businesses. Small business vendors are routed to the FEMA Small Business Analyst for notification, support and processing. For more information see http://www.fema.gov/privatesector/industry/about.shtm or contact FEMA-SB@dhs.gov.

FEMA Think Tank In 2012, FEMA launched a collaborative forum to engage our partners, promote innovation, and facilitate discussions in the field of emergency management. This forum is open to the whole community: state, local, and tribal governments, as well as all members of the public, including the private sector, the disability community, and volunteer community. The primary goal is to seek their input on how to improve the emergency management system, explore best practices and generate new ideas. The FEMA Think Tank has two main components:

- **Online Forum:** Visitors can submit their own ideas, comment on others, and participate in conversations meant to generate creative solutions. The forum is open to anyone who wants to discuss a variety of emergency management issues, such as how we prepare for, respond to, recover from, or mitigate against all types of disasters, as well as ideas on how we can continue to integrate the whole community. (http://fema.ideascale.com/)
- **Monthly Conference Call Discussions:** Deputy Administrator Richard Serino held the first monthly conference call in January 2012, to discuss some of the real-life solutions and ideas that are generated by this online forum. These calls are open to the general public, with captioning for participants who are deaf or hard of hearing. The Deputy Administrator travels to a different location each month to personally meet with members of the emergency management community. To find out when the next call will be, see http://www.fema.gov/thinktank/conferencecalls.shtm.

The **Homeland Security Advisory Council (HSAC)** provides advice and recommendations to the Secretary of Homeland Security on matters related to homeland security. The Council is comprised of 30 members selected by the Secretary that are leaders from State and local government, first responder communities, the private sector, and academia. The Council is an independent, bipartisan advisory board of leaders that recently produced reports on border security, countering violent extremism, community resilience, sustainability and efficiency, and the previous Homeland Security Advisory System. For more information or to apply to be a member, please visit http://www.dhs.gov/files/committees/editorial_0331.shtm or contact at hsac@dhs.gov.

ICE Office of Public Affairs (OPA) is dedicated to building understanding and support for the agency mission through outreach to employees, the media and the general public. ICE field public affairs officers are stationed throughout the country and are responsible for regional media relations in specific geographic areas. For more information, see http://www.ice.gov or contact PublicAffairs.ICEOfficeOf@dhs.gov, or (202) 732-4242.

National Infrastructure Protection Plan (NIPP) Sector Partnership improves the protection and resilience of the nation's critical infrastructure sectors. The partnership provides a forum for 18 designated, critical sectors to engage with the federal government regularly on national planning, risk mitigation program identification and implementation, and information sharing. Additional information for private sector owners and operators of critical infrastructure may be found at www.dhs.gov/criticalinfrastructure or contact Sector.Partnership@dhs.gov.

Office of Small and Disadvantaged Business Utilization (OSDBU) serves as the focal point for small business acquisition matters and works closely with all DHS Components. OSDBU makes available forecasts of contract opportunities, vendor outreach sessions, lists of component small business specialists, DHS prime contractors, and information about the DHS mentor-protégé program. For more information, see http://www.dhs.gov/openforbusiness or contact OSDBU, (202) 447-5555.

Private Sector Updates The DHS Private Sector Office sends weekly e-mails with homeland security news and resources to our private sector partners. To ensure that your organization has the most up to date information on homeland security related private sector information, visit https://service.govdelivery.com/service/subscribe.html?code=USDHS_99. For more information, contact private.sector@dhs.gov or (202) 282-8484.

Private Sector for a Day Following the success of the DHS for a Day program, the DHS Private Sector Office launched this program in 2012 for partners from across the federal government to engage meaningfully with relevant experts in the private sector and to learn from private sector best practices on issues ranging from social media to cybersecurity. For more information, email private.sector@dhs.gov.

Private Sector Representative in the National Response Coordination Center One of the most innovative programs at FEMA is one in which FEMA opens its doors to peers from the private sector for 90 days at a time. During this rotation, the Private Sector Representative is a special government employee representing the broad private sector (not just the home organization) and works side-by-side with us during normal operations and during disasters. The program started in 2011, and has included both Fortune 500 companies and small business. It is also open to academia and other segments of the private sector. Email FEMA-PSR@fema.dhs.gov.

Private Sector Division/Office of External Affairs FEMA established a Private Sector Division within the Office of External Affairs in October 2007. The division's purpose is to communicate, cultivate and advocate for collaboration between the U.S. private sector and FEMA, to support FEMA's capabilities and to enhance national preparedness, protection, response, recovery, and mitigation of all hazards. The division's vision is to establish and maintain a national reputation for effective support to our private sector stakeholders through credible, reliable and meaningful two-way communication. Fema-private-sector@dhs.gov; www.fema.gov/privatesector

Regional and Disaster Private Sector Liaisons In addition to the headquarters team, FEMA designated a private sector liaison in each of its 10 regions to cultivate two-way communication between FEMA, state/local/tribal/territorial officials, and private sector during steady state and disaster operations. During disasters, a reserve cadre of private sector specialists deploys to support Joint Field Office efforts, as part of ESF 15- External Affairs. For more information, please contact fema-private-sector@dhs.gov.

Sector-Specific Agency (SSA) for Communications The National Communications System (NCS) is the SSA for Communications under Homeland Security Presidential Directive 7 (HSPD-7). Under the National Infrastructure Protection Plan (NIPP) structure, there is a Government Coordinating Council (GCC) and a Sector Coordinating Council (SCC) that work to reduce risk across the Communications Sector. This resource is helpful in assisting in coordinating risk-based critical infrastructure plans and programs to address known and potential hazards, to incorporate lessons learned and best practices into operational and contingency plans, and to identify and address dependencies and interdependencies to allow for more timely and effective implementation of short-term protective actions. For more information, contact cipac@dhs.gov.

Telecom / Energy Working Group was created by the Communications Government Coordinating Council to follow up on the Communications Dependency on Electric Power Working Group Report recommendations. The Working Group's mission is to protect the nation's telecommunications critical infrastructure against long-term electric power outages. For more information, contact brice.hall@hq.dhs.gov.

Policy Guidance

American National Standards Institute – Homeland Security Standards Database (ANSI-HSSD) provides a single, comprehensive source for standards that relate to homeland security. To meet this goal, ANSI partnered with DHS, standards developing organizations, and other stakeholders to identify and classify those standards that are pertinent to the area of homeland security. This effort deals with the area of first responders and was organized in cooperation with the Responder Knowledge Base and uses the Standardized Equipment List (SEL) from the Interagency Board as the basis for the classification structure. For more information see www.hssd.us/ or contact Michelle Maas Deane, Director, Homeland Security Standards, ANSI (mdeane@ansi.org).

American National Standards Institute – Homeland Security Standards Panel (ANSI-HSSP) identifies existing consensus standards, or, if none exist, assists DHS and sectors requesting assistance to accelerate development and adoption of consensus standards critical to homeland security. The ANSI-HSSP promotes a positive, cooperative partnership between the public and private sectors in order to meet the needs of the nation in this critical area. Participation in the ANSI-HSSP is open to representatives of industry, government, professional societies, trade associations, standards developers, and consortia groups directly involved in U.S. Homeland Security standardization. For additional information visit www.ansi.org/hssp or contact Michelle Maas Deane, Director, Homeland Security Standards, ANSI (mdeane@ansi.org).

2011 National Sector Risk Assessment (NSRA) is a joint public-private initiative to reduce risk to, and increase the resilience of, the communications sector. The Office Manager National Communications System (OMNCS) and its government and private sector partners, under Homeland Security Presidential Directive 7 and the National Infrastructure Protection Plan, are updating the 2008 NSRA as part of the 2011 NSRA. The 2011 NSRA will be a series of communications sector risk assessment reports consisting of a review, analysis, and update. For more information, please email will.williams@dhs.gov or julian.humble@dhs.gov.

International Issues for Critical Infrastructure and Key Resources (CIKR) Protection This two-page snapshot describes the approach to international issues embodied in the NIPP and the Sector-Specific Plans. The National Infrastructure Protection Plan (NIPP) brings a new focus to international security cooperation and provides a risk-based framework for collaborative engagement with international partners and for measuring the effectiveness of international CIKR protection activities. For more information, see http://www.dhs.gov/xlibrary/assets/nipp_international.pdf or contact NIPP@dhs.gov.

IS-821 Critical Infrastructure Support Annex is an independent study course that provides an introduction to the Critical Infrastructure Support Annex to the National Response Framework. See http://training.fema.gov/emiweb/is/is821.asp, for more information, contact IP_Education@hq.dhs.gov.

IS-860.a National Infrastructure Protection Plan (NIPP) is an Independent Study course that presents an overview of the NIPP. The NIPP provides the unifying structure for the integration of existing and future critical infrastructure protection and resiliency efforts into a single national program. This course has been updated to align with the NIPP that was released in 2009. Classroom materials are also available for this course. For more information, visit http://training.fema.gov/emiweb/is/is860a.asp or contact IP_Education@hq.dhs.gov.

IS-890.a Introduction to the Interagency Security Committee (ISC) is the first course in the independent study ISC web-based training series. The purpose of this series of courses is to provide federal facility security professionals, engineers, building owners, construction contractors, architects, and the general public with basic information pertaining to the ISC and its facility security standards, processes, and practices. This course provides an overview of the history of the ISC, its mission and organization, and a basic outline of the ISC risk management process. The course can be accessed at: http://training.fema.gov/EMIWeb/IS/is890a.asp. For more information contact Isc@dhs.gov.

Guide to Critical Infrastructure Protection at the State, Regional, Local, Tribal, & Territorial Level(2008) outlines the attributes, capabilities, needs, and processes that a state or local government entity should include in establishing its own critical infrastructure protection function that integrates with the National Infrastructure Protection Plan (NIPP) and accomplishes the desired local benefits. To download this document visit http://www.dhs.gov/xlibrary/assets/nipp_srtltt_guide.pdf or contact NIPP@dhs.gov.

Infrastructure Protection Report Series (IPRS) is a comprehensive series of For Official Use Only (FOUO) reports containing detailed information for all 18 Critical Infrastructure and Key Resources (CIKR) sectors focusing on infrastructure characteristics and common vulnerabilities, potential indicators of terrorist activity, potential threats, and associated protective measures. The IPRS is available to vetted private sector critical infrastructure owners and operators with a demonstrated need to know through the Homeland Security Information Network-Critical Sectors (HSIN-CS) (https://cs.hsin.gov/) online secure portal. For more information on the IPRS, critical infrastructure private sector owners and operators should contact IPassessments@hq.dhs.gov.

National Incident Management System (NIMS) provides a systematic, proactive approach to guide departments and agencies at all levels of government, nongovernmental organizations, and the private sector to work seamlessly to prevent, protect against, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or complexity, in order to reduce the loss of life and property and harm to the environment. For more information, see www.fema.gov/nims. Questions regarding NIMS should be directed to FEMA-NIMS@dhs.gov or (202) 646-3850.

National Infrastructure Protection Plan (NIPP) 2009 provides the unifying structure for the integration of a wide range of efforts for the enhanced protection and resilience of the Nation's critical infrastructure into a single national program. For more information, see http://www.dhs.gov/files/programs/editorial_0827.shtm or to request materials contact NIPP@dhs.gov.

National Response Framework (NRF) is a guide to how the nation conducts all-hazards response. It is built upon scalable, flexible, and adaptable coordinating structures to align key roles and responsibilities across the nation, linking all levels of government, nongovernmental organizations, and the private sector. It is intended to capture specific authorities and best practices for managing small- or large-scale incidents, terrorist attacks or catastrophic natural disasters. For more information, visit http://www.fema.gov/nrf.

NIPP in Action Stories are multi-media pieces highlighting successes in National Infrastructure Protection Plan (NIPP) and Sector Specific Plan (SSP) implementation; these stories can take the form of a printed snapshot, a short video, or a poster board. NIPP in Action stories are developed in concert with sector partners and are designed to promote cross-sector information sharing of best practices with government partners and infrastructure owners and operators. If you would like more information or are interested in developing a NIPP in Action story, contact NIPP@dhs.gov.

Office of Infrastructure Protection (IP) and National Infrastructure Protection Plan (NIPP) Booths are available for exhibition at national and sector-level events to promote awareness of the IP mission and the NIPP to government partners and infrastructure owners and operators. In addition, IP maintains a cadre of trained speakers who are available to speak on critical infrastructure protection and resilience issues at conferences and events. For more information, contact IP_Education@hq.dhs.gov.

Physical Security Criteria for Federal Facilities: An Interagency Security Committee Standard (FOUO) This document is a new interim ISC standard. The standard establishes a baseline set of physical security measures to be applied to all federal facilities based on their designated facility security level. It also provides a framework for the customization of security measures to address unique risks faced at each facility. The interim standard will be used during a 24-month validation period to confirm the need and usability of this standard. For more information, please contact the NPPD/IP ISC at ISC@dhs.gov.

Sector Annual Reports (FOUO) The SSPs provide the means by which the NIPP is implemented across all critical infrastructure sectors. Each Sector-Specific Agency is responsible for developing and implementing an SSP through a coordinated effort involving their public and private sector critical infrastructure partners. Collaborating with government and private sector to develop, update, and maintain Sector Annual Reports for the Chemical, Commercial Facilities, Critical Manufacturing, Dams, Emergency Services, and Nuclear Sectors. For more information please contact SOPDExecSec@dhs.gov

Sector-Specific Plans SSPs support the National Infrastructure Protection Plan (NIPP) by establishing a coordinated approach to national priorities, goals, and requirements for critical infrastructure protection. Each SSP provides the means by which the NIPP is implemented for each sector, as well as a national framework to address the sector's unique characteristics and risk landscape. Copies of the 2010 SSPs that are not marked FOUO can be downloaded at: http://www.dhs.gov/files/programs/gc_1179866197607.shtm.

State and Local Implementation Snapshot In accordance with the National Infrastructure Protection Plan (NIPP), as well as the requirements identified in the Homeland Security Grant Program, State and tribal governments are responsible for developing, implementing, and sustaining a statewide/regional critical infrastructure protection program. The processes necessary to implement the NIPP risk management framework at the state and/or regional level, including urban areas, should become a component of the state's overarching homeland security program. This two-page snapshot presents information on a variety of resources available to support State/local and tribal critical infrastructure protection efforts. For more information, see http://www.dhs.gov/xlibrary/assets/nipp_state_local_snapshot.pdf.

Research and Product Development

The **Acquisition Planning Forecast System (APFS)** provides the DHS Forecast of Contract Opportunities in accordance with Public Law 100-656, Section 501. The Forecast data is for planning purposes and is not a commitment by the government to purchase the desired products and services. Please note that the contact information in this system is provided to the vendor community for the specific requirements identified in each potential contract action. Use of contact information for the purpose of mass distribution of marketing materials unrelated to a specific need is improper use of the system. The search screen below is provided for your use in locating potential future contract actions. http://apfs.dhs.gov/

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

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

Commercialization Office develops and executes programs and processes that identify, evaluate, and commercialize technologies into products or services that meet the detailed operational requirements of DHS stakeholders. The Commercialization Office also spearheads DHS Science and Technology Directorate outreach efforts to inform the private sector on doing business with DHS. For more information, see http://www.dhs.gov/xabout/structure/gc_1234194479267.shtm. Contact: SandT_Commercialization@hq.dhs.gov, (202) 254-6749.

Defense Technology Experimental Research (DETER) is a national cyber-security experimental infrastructure which enables users to study and evaluate a wide range of computer security technologies including encryption, pattern detection, intrusion tolerant storage protocols, next generation network simulations; as well as, develop and share educational material and tools to train the next generation of cyber-security experts. Newsletters, published papers, videos and presentations can be viewed at http://www.isi.edu/deter/ or contact testbed-ops@isi.deterlab.net.

DHS Technology Transfer Program promotes the transfer and/or exchange of technology with industry, state and local governments, academia, and other federal agencies. The technologies developed and evaluated within DHS can have potential commercial applications and dramatically enhance the competitiveness of individual small businesses as well as expanding areas of cooperation for non-federal partners. For more information, visit http://www.dhs.gov/xabout/structure/gc_1264538499667.shtm.

DHS Small Business Innovation Research (SBIR) Program is designed to: stimulate technological innovation; strengthen the role of small business in meeting DHS research and development needs; foster and encourage participation of socially and economically disadvantaged persons and women-owned small business concerns in technological innovation; and increase the commercial application of DHS-supported research or research and development results. SBIR research areas are chosen for their applicability to support homeland security missions and address the needs of the seven DHS operational units. Additional information can be found at https://www.sbir.gov.

FutureTECH™ targets critical research/innovation focus areas to communicate to the private sector and national labs the long-term needs of the Department. For more information, see http://www.dhs.gov/files/programs/gc_1242058794349.shtm or contact SandT_Commercialization@hq.dhs.gov, (202) 254-6749.

Homeland Open Security Technologies works to improve federal, state, and local government's ability to collaborate with the open source software communities focused on security. The objectives are to improve the process for government acquisition of open technology, encourage the contribution of government funded research to the communities, and identify and seed development in prioritized gaps. http://www.cyber.st.dhs.gov/host/.

Long Range Broad Agency Announcement (LRBAA) is an acquisition instrument for research and development projects which address DHS capability gaps or advance technical knowledge in the basic sciences. The LRBAA is not a procurement mechanism for mature products or concepts. Rather, successful submissions answer questions such as, "What research problem do you propose to solve? How is your solution different from and superior to currently available solutions or from the efforts of others to achieve a similar solution? What data and analysis do you have to support the contention that funding your R&D project will result in a significant increase in capability for DHS?" For submission instructions, evaluation criteria, research topics, and to apply online, visit: https://baa2.st.dhs.gov.

Mass Transit Security Technology Testing In coordination with TSA's Office of Security Technology and DHS's Office of Science and Technology, the Mass Transit Division pursues development of multiple technologies to advance capabilities to detect and deter terrorist activity and prevent attacks. TSA partners with mass transit and passenger rail agencies to conduct pilot testing of various security technologies. These activities evaluate these capabilities in the varied operational environments that prevail in rail and bus operations across the country. For more information, contact MassTransitSecurity@dhs.gov.

National Urban Security Technology Laboratory (NUSTL) tests, evaluates, and analyzes homeland security capabilities while serving as a technical authority to first responder, state, and local entities.

NUSTL is a federal technical resource supporting the successful development, integration, and transition of homeland security technologies into operational end-user environments. NUSTL's broad ranging relationships with the homeland security community enable the use of the New York metropolitan area as an urban test bed for the diverse technologies and systems being developed to prepare and protect our nation. For more information, contact nustl@dhs.gov.

Planning Guidelines and Design Standards (PGDS) for Checked Baggage Inspection Systems incorporate insights and experience of industry stakeholders, including airport and airline representatives, planners, architects, baggage handling system designers, and equipment manufacturers. The PGDS assists planners and designers in developing cost-effective solutions and to convey TSA requirements for checked baggage inspection systems. The PGDS emphasizes best practices associated with screening system layouts and addresses other factors necessary to actively manage system costs and performance. For more information, see http://www.tsa.gov/press/happenings/updated_pgds.shtm or contact the TSA Contact Center, (866) 289-9673.

Project 25 Compliance Assessment Program (P25 CAP) was established, in coordination with the National Institute of Standards and Technology (NIST), to provide a process for ensuring that equipment complies with P25 standards, meets performance requirements, and is capable of interoperating across manufacturers. P25 CAP allows emergency responders to confidently purchase and use P25-compliant products. For more information, see http://www.pscr.gov/projects/lmr/p25_cap/p25_cap.php or contact P25CAP@dhs.gov.

Research and Standards Integration Program (RSI) interfaces with public and private sector organizations to advance the future state of cybersecurity through Research and Development (R&D) and standards for information and communications technology. RSI seeks input from academic and industry researchers to determine if their R&D projects map to CS&C R&D requirements, particularly to identify relevant federally funded research in areas such as visualization for cybersecurity, enterprise-level situational awareness, and analytic frameworks. For more information, contact RSI@hq.dhs.gov.

Science & Technology Basic Research Focus Areas represent the technological areas in which S&T seeks to create and/or exploit new scientific breakthroughs and help guide the direction of the S&T research portfolio and to provide long-term science and technology advances for the benefit of homeland security. The focus areas identified by the S&T Research Council, with input from customers and the research community, summarize the fundamental work needed to support the future protection of our nation. Contact the Director of Research, SandT.Research@dhs.gov , and (202) 254-6068.

SECURE™ Program leverages the experience and resources of the private sector to develop fully deployable products/services based on Department generated and vetted, detailed commercialization-based operational requirements documents and a conservative estimate of the potential available market of Department stakeholders. For more information, see http://www.dhs.gov/files/programs/gc_1211996620526.shtm, or contact sandt_commercialization@hq.dhs.gov, (202) 254-6749.

Support Anti-Terrorism by Fostering Effective Technologies Act (SAFETY Act) evaluates and qualifies technologies for liability protection in accordance with the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act of 2002 and the supporting regulations of the Final Rule (6 CFR Part 25) implemented on July 10, 2006. The SAFETY Act provides risk management and liability protections for sellers of Qualified Anti-Terrorism Technologies. The purpose of the SAFETY Act is to ensure that the threat of liability does not deter potential manufacturers or sellers of effective anti-terrorism technologies from developing, deploying and commercializing these technologies that meet homeland security objectives. For more information, see www.SAFETYAct.gov or contact SAFETYActHelpDesk@dhs.gov, (866) 788-9318.

System Assessment and Validation for Emergency Responders (SAVER) Program assists responders making procurement decisions by conducting objective operational assessments and technical verifications of commercially available responder equipment. SAVER provides those results along with other relevant equipment information to the responder community in an operationally useful form. SAVER provides information that enables decision-makers and responders to better select, procure, use, and maintain emergency responder equipment. More information and copies of SAVER reports can be obtained at: https://www.rkb.us/saver or by contacting SAVER at SAVER@dhs.gov.

The TechSolutions Program provides information, resources and technology solutions that address mission capability gaps identified by the emergency response community. The goal of TechSolutions is to field technologies that meet at least 80% of the operational requirement, in a 12 to 15 month timeframe, at a cost commensurate with the proposal. Goals will be accomplished through rapid prototyping or the identification of existing technologies that satisfy identified requirements. For more information, see www.firstresponder.gov or www.techsolutions.dhs.gov.

Transportation Security Laboratory (TSL) conducts applied research, development, integration, and validation of cutting edge science and technology solutions for the detection and mitigation of explosives and conventional weapons. More specifically its core capabilities are: Ability to characterize, categorize, maintain, and enhance understanding of the wide array of explosives and energetic materials found throughout the world; develop, maintain, and enhance the DHS position as technical experts in understanding state-of-the-art science and technology in all fields related to explosives detection, response, and mitigation; and to maintain a leadership role in independent test and evaluation of technologies prior to field deployment including an independent and objective certification/qualification process for technologies. For more information, contact tslinfo@dhs.gov.

Protecting Against Fraud & Counterfeiting

Anti-Piracy Public Service Announcement The National Intellectual Property Rights Coordination Center (IPR Center) is the U.S. Government clearinghouse for investigations into counterfeiting and piracy. The IPR Center takes an active role in combating piracy both online and in the real world. Accordingly, the IPR Center endeavors to educate the general public about the consequences of IP theft and has released a public service announcement designed to discourage consumers from buying pirated content. For more information, see http://www.ice.gov/doclib/flash/videos/nyc-antipiracy.swf.

CBP Directives Pertaining to Intellectual Property Rights are policy guidance documents that explain CBP legal authority and policies implementing certain laws and regulations. They are distributed to CBP personnel to clarify implementation procedures and are made available to the public to explain CBP's policies. To access these directives, visit http://www.cbp.gov/xp/cgov/trade/legal/directives/ or contact iprpolicyprograms@dhs.gov.

Commercial Fraud ICE Homeland Security Investigations (HSI) investigates commercial fraud, including false statements and deceptive business practices. The ICE HSI Commercial Fraud Programs Unit, which is led by the IPR Center, prioritizes health and safety violations, U.S. economic interests, and duty collection. For more information, see http://www.iprcenter.gov/reports/fact-sheets/commercial-fraud/view.

eInformation Network The Secret Service eInformation Network is available – for free – to authorized law enforcement officers, financial institution investigators, academic partners, and commercial partners of the Secret Service. The site contains three 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; an Electronic Crimes Task Force component that serves as an efficient, secure web-based collection of best practices, vulnerability guides, National Infrastructure Protection Center (NIPC) advisories, and a subject-specific issue library; and the US Dollars Counterfeit Note Search, a site that provides the user with the ability to conduct a search of the Secret Service counterfeit note database. For more information, see www.einformation.usss.gov.

Electronic Crimes Task Force (ECTF) Program brings together not only federal, state and local law enforcement, but also prosecutors, private industry and academia. The common purpose is the prevention, detection, mitigation and aggressive investigation of attacks on the nation's financial and critical infrastructures. The U.S. Secret Service's ECTF and Electronic Crimes Working Group initiatives prioritize investigative cases that involve electronic crimes. These initiatives provide necessary support and resources to field investigations that meet any one of the following criteria: significant economic or community impact, participation of organized criminal groups involving multiple districts or transnational organizations, or the use of schemes involving new technology. For more information, see http://www.secretservice.gov/ectf.shtml.

Financial Crimes Task Forces (FCTF) combines the resources of the Secret Service, state and local law enforcement, and the financial industry to combat financial crimes. The technological advance of domestic and transnational criminals allows new avenues to exploit financial institutions, thus making internationally-based criminal enterprises even more problematic for law enforcement. The most effective means of combating organized criminal elements, both in the U.S. and abroad, is through the use of Financial Crimes Task Forces. The multi-agency components are well suited to conduct complex, in-depth, multi-jurisdictional investigations. For more information contact your local Secret Service field office at www.secretservice.gov/field_offices.shtml.

How to Protect Your Rights The flow of counterfeit and pirated goods is a global problem that requires vigorous collaboration between customs agencies and rights owners to ensure effective intellectual property enforcement at the border. Working with CBP provides many benefits for rights owners of patents, copyrights, and trademarks to ensure maximum intellectual property rights protection. The three steps you can take to maximize your relationship with CBP are e-Recordation, e-Allegations, and information sharing. For more information, visit http://www.cbp.gov/linkhandler/cgov/trade/priority_trade/ipr/legal/ipr_guide.ctt/ipr_guide.pdf.

HSI Illicit Finance and Proceeds of Crime Unit (IFPCU) ICE recognizes that the private sector represents America's first line of defense against money laundering. With IFPCU, ICE Homeland Security Investigations reaches out to the U.S. business community, along with state and federal agencies to combat financial and trade crimes. IFPCU identifies and eliminates vulnerabilities within the U.S. financial, trade and transportation sectors--vulnerabilities that criminal and terrorist organizations could exploit to finance their illicit operations and avoid being detected by law enforcement. The IFPCU publishes the Cornerstone Report, a quarterly newsletter. This report provides current trends and financial crimes identified by law enforcement and the private sector. To subscribe to the Cornerstone Report, or for more information, see www.ice.gov/cornerstone or call (866) DHS-2-ICE (866-347-2423).

ICE HSI National Security Investigations Division ICE is involved in almost every foreign terrorism investigation related to cross-border crime. Foreign terrorists need to move money, weapons and people across international borders to conduct their operations, and ICE holds a unique set of law enforcement tools for disrupting these illicit activities. ICE HSI's National Security Investigations Division, integrates the agency's national security investigations and counter-terrorism responsibilities into a single overarching division. To report suspicious activity, call 1-866-DHS-2-ICE (1-866-347-2423) or complete ICE HSI's online tip form at http://www.ice.gov/exec/forms/hsi-tips/tips.asp

Intellectual Property Rights (IPR) Fact Sheet U.S. Customs and Border Protection (CBP) enforces IPR, most visibly by seizing products that infringe IPR such as trademarks, copyrights, and patents. The theft of intellectual property and trade in fake goods threaten America's economic vitality and national security, and the American people's health and safety. For more information, please visit http://www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/trade/ipr_fact_sheet.ctt/ipr_fact_sheet.pdf

Intellectual Property Rights (IPR) and Restricted Merchandise Branch oversees the IPR recordation program and provides IPR infringement determinations and rulings. For more information, contact hqiprbranch@dhs.gov or call (202) 325-0020.

Intellectual Property Rights (IPR) Continuous Sample Bond is a continuous bond option for Intellectual Property Rights (IPR) sample bonds. Under CBP regulations, CBP may provide samples of certain merchandise suspected of bearing infringing trademarks, trade names, or copyrights of imports seized for such violations, to trademark, trade name, and copyright owners. For additional information, contact cbp.bondquestions@dhs.gov, or (317) 614-4880.

Intellectual Property Rights (IPR) Enforcement: A Priority Trade Issue The trade in counterfeit and pirated goods threatens America's innovation economy, the competitiveness of our businesses, the livelihoods of U.S. workers, national security, and the health and safety of consumers. The trade in these illegitimate goods is associated with smuggling and other criminal activities, and often funds criminal enterprises. For more information, visit www.cbp.gov/ipr.

Intellectual Property Rights (IPR) e-Recordation and IPR Search The first step in obtaining IPR protection by CBP is to record validly registered trademarks and copyrights with CBP through the Intellectual Property Rights e-Recordation (IPRR) online system. The CBP on-line recordation allows intellectual property owners to electronically record their trademarks and copyrights with CBP, and makes IPR recordation information readily available to CBP personnel, facilitating IPR seizures by CBP. CBP uses recordation information to actively monitor shipments and prevent the importation or exportation of infringing goods. For more information, see http://iprs.cbp.gov/ or contact hqiprbranch@dhs.gov (202) 325-0020.

Intellectual Property Rights (IPR) Help Desk can provide information and assistance for a range of IPR related issues including: IPR border enforcement procedures, reporting allegations of IPR infringement, assistance for owners of recorded IPRs to develop product identification training materials, and to assist officers at ports of entry in identifying IPR infringing goods. For more information, contact ipr.helpdesk@dhs.gov or (562) 980-3119 ext. 252.

Intellectual Property Rights (IPR) Seizure Statistics CBP maintains statistics on IPR seizures made by the DHS. For more information, see http://www.cbp.gov/xp/cgov/trade/priority_trade/ipr/ipr_communications/seizure/ or contact iprpolicyprograms@dhs.gov or ipr.helpdesk@dhs.gov.

IPR Product Identification Guide Organizations that are concerned about intellectual property violations at America's borders may submit a Product Identification Guide that will easily allow CBP Officers to determine which products are genuine and which are counterfeit. For more information, see http://www.cbp.gov/xp/cgov/trade/priority_trade/ipr/legal/training_guide/

National Intellectual Property Rights Coordination Center (IPR Center) is a task force that uses the expertise of its member agencies to share information, develop initiatives, coordinate enforcement actions, and conduct investigations related to intellectual property theft. Through this strategic interagency partnership, the IPR Center protects public health and safety, the U.S. economy, and the war fighters. If a company has specific information concerning IP theft, it can send an email to IPRCenter@dhs.gov, visit www.iprcenter.gov, or call 866-IPR-2060. For more information on the IPR center, see http://www.iprcenter.gov/reports/fact-sheets/national-intellectual-property-rights-ipr-coordination-center-ipr-investigations.

Operation Genesis is a voluntary partnership with the printing industry to share information and develop investigative leads regarding the practices of organized document fraud rings. Operation Genesis affords an opportunity for the printing industry to collaborate with ICE to identify and disrupt document fraud. Information available to Operation Genesis interested parties include a broad based introductory brochure. For more information, contact IBFU-ICE-HQ@DHS.GOV.

Operation Guardian is a multi-agency effort to combat the increasing importation of substandard, tainted, and counterfeit products that pose a health and safety risk to consumers. The identification of these commodities has led to the successful detention and seizure of numerous containers of hazardous products. For more information, visit http://www.iprcenter.gov/reports/fact-sheets/Operation%20Guardian%20Fact%20Sheet%20FINAL%20-%20IPR%20DIRECTOR%20APPROVAL.pdf/view.

Operation In Our Sites specifically targets websites and their operators that distribute counterfeit and pirated items over the Internet, including counterfeit pharmaceuticals and pirated movies, television shows, music, software, electronics, and other merchandise, as well as products that threaten public health and safety. For more information, visit http://www.ice.gov/doclib/news/library/factsheets/pdf/operation-in-our-sites.pdf.

Report an IPR Violation In furtherance of the U.S. Government's IPR enforcement efforts, the IPR Center continues to encourage the general public, industry, trade associations, law enforcement, and government agencies to report violations of intellectual property rights. To better facilitate IP theft reporting, the IPR Center created an "IP Theft Button." As a result, anyone in the world with Internet access has the capability to report an IPR violation and provide information directly to the IPR Center for investigative consideration. If a company or individual has specific information concerning IP theft, they can send an email to IPRCenter@dhs.gov, visit www.iprcenter.gov, call (866) IPR-2060, or click on the IP Theft Button now available on U.S. Embassy, U.S. Consulate, private industry, and trade association websites worldwide. http://www.iprcenter.gov/reports/Reporting%20Allegations%20of%20Intellectual%20Property%20Theft%20Brochure.pdf/view

Social Media Engagement

The Blog @ Homeland Security provides an inside-out view of what we do every day at DHS. The Blog lets us talk about how we secure our nation, strengthen our programs, and unite the Department behind our common mission and principles. It also lets us hear from you. For more information, visit http://blog.dhs.gov.

Coast Guard Blogs and News For a discussion forum on Marine Safety, Recreational Boating Safety, and waterways management as we work together to protect maritime commerce and mobility, the marine environment, and safety of life at sea, visit http://cgmarinesafety.blogspot.com, http://harborsafetycommittee.blogspot.com/, www.uscgnews.com, or www.twitter.com/uscoastguard.

CRCL's Facebook Page allows our Office to instantly connect with the public and share information about our work supporting the Department to secure the nation while preserving individual liberty, fairness, and equality under the law. Through our Facebook page, we share important information about DHS programs and policies and engage with our "friends" to receive feedback, and learn about civil rights and civil liberties issues occurring in communities throughout the country. "Like" our page, and start a conversation.

DHS Social Media Engagement The Department of Homeland Security is using "Web 2.0," social media technologies and Web sites to provide you with information in more places and more ways. For a full list of DHS Facebook pages, twitter feeds, blogs, and other social media resources, see http://www.dhs.gov/xabout/gc_1238684422624.shtm.

USCIS Social Media tools both provide information to and engage in discussions with the public. These tools include The Beacon – The official blog of USCIS -at www.uscis.gov/blog; Twitter channels in both English www.twitter.com/uscis and Spanish www.twitter.com/uscis_es; and a YouTube channel for hosting video content www.youtube.com/uscis

FEMA Private Sector Web Portal aggregates FEMA online resources for the private sector. Content includes promising practices in public-private partnerships, weekly preparedness tips, links to training opportunities, planning and preparedness resources, information on how to do business with FEMA, and more. For more information, see www.fema.gov/privatesector.