Private Sector Resources Catalog

May 2010

Homeland Security

Intentionally blank page. Please continue to the next page.

Contents

Letter from Assistant Secretary Douglas A. Smith

May 10, 2010

Dear Private Sector Partner,

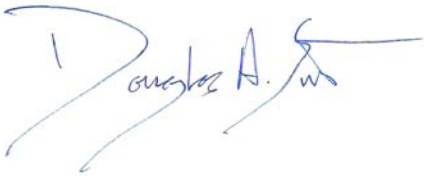
To better facilitate your organization's access to the resources you need to help keep our country secure, DHS has developed this catalog. The first to be targeted specifically towards private sector partners and encompass all of DHS, this document collects the training, publications, guidance, alerts, newsletters, programs, and services available to the private sector across the department. It is organized by component and resource type and a comprehensive index is available to facilitate locating resources. Additionally, contact information across the department is available in Appendix A. Recognizing the diversity of the available resources as well as the continually evolving work of the department, this catalog will be updated regularly to publicize new resources and to increase private sector awareness.

In order to face the new threats and evolving hazards of today's security environment, we must develop and maintain critical homeland security capabilities at all layers of our society. We all share the responsibility to build all-hazards preparedness and resiliency into our way of life. As outlined in the Quadrennial Homeland Security Review Report released earlier this year, this *enterprise* approach is composed of multiple partners whose roles and responsibilities are distributed and shared among a broad-based community with a common interest in the public safety and well-being of America and American society.

The private sector is a critical partner in our homeland security efforts and my office is committed to strengthening the Department's relationship with organizations such as yours. As primary advisor to the Secretary on issues related to the private sector, including academia, non-profits, NGOs, and businesses, the Private Sector Office (PSO) coordinates active engagement between DHS and the private sector.

Regardless of where your organization fits into the homeland security enterprise, the Private Sector Office is committed to providing you with the assistance and support you require. You can contact our office at any time with requests, comments, questions, issues or concerns at private.sector@dhs.gov, (202) 282-8484.

Sincerely,



Douglas A. Smith
Assistant Secretary for the Private Sector

Department-wide Resources

The Blog @ Homeland Security provides an inside-out view of what we do every day at the U.S. Department of Homeland Security. 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. Visit http://www.dhs.gov/journal/theblog/.

Commercialization Office is responsible for the development and implementation of a commercialization process and for the execution of two innovative public-private partnerships that leverage research and development efforts in the private sector that are aligned to detailed operational requirements from Department stakeholders. The Commercialization Office also spearheads DHS Science and Technology's (S&T) outreach efforts that inform the private sector on "How to do business with DHS." See http://www.dhs.gov/xabout/structure/gc_1234194479267.shtm. Contact: SandT_Commercialization@hq.dhs.gov, 1-(202) 254-6749.

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. See http://www.federallabs.org or contact FLETC-CRADAProgramOffice@dhs.gov, (912) 267-2100.

DHS Center for Faith-Based and Community Initiatives (CFBCI) builds, sustains, and improves effective partnerships between government sectors and faith-based and community organizations. Located within FEMA, CFBCI 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 Office of Infrastructure Protection (IP) leads the national effort to mitigate risk to America's critical infrastructure from the full spectrum of 21st Century threats and hazards. IP coordinates with government and critical infrastructure owners and operators across 18 diverse sectors to enhance critical infrastructure resilience, strengthen protective programs, and share vital information. For more information on IP programs and resources visit www.dhs.gov/criticalinfrastructure.

DHS Private Sector Office As primary advisor to the Secretary on issues related to the private sector, including academia, non-profits, NGOs, and businesses, the Private Sector Office coordinates active engagement between DHS and the private sector to build strong partnerships, shape policy, and enhance internal and external dialog. For more information, contact the private sector office at private.sector@dhs.gov, (202) 282-8484.

DHS Private Sector Community Preparedness Updates The DHS Private Sector Office sends a weekly update e-mail collecting homeland security news and resources. To subscribe, see https://service.govdelivery.com/service/subscribe.html?code=USDHS_99. For more information, contact private.sector@dhs.gov, (202) 282-8484.

DisabilityPreparedness.gov is the Disability Resource Center of the Interagency Coordinating Council on Emergency Preparedness and Individuals with Disabilities (ICC). Maintained by the DHS Office for Civil Rights and Civil Liberties (CRCL), this site is the main repository for information related to the activities of the ICC, including bimonthly updates regarding federal programs and services relevant to individuals with disabilities and emergency preparedness. The site also contains information to assist individuals with disabilities in personal preparedness planning; provides emergency managers, first responders, and other disaster service providers with resources relevant to working with individuals who have disabilities; and offers tips regarding how individuals with disabilities can get involved in preparedness activities within their communities. This resource can be accessed at www.disabilitypreparedness.gov. For more information, contact Disability.preparedness@dhs.gov, (202) 357-8483.

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

E-Verify and Unfair Labor Practices The DHS Office for Civil Rights and Civil Liberties (CRCL) staff provides training on the responsibilities imposed upon the private sector when using E-Verify. Training includes best practices, examples of unlawful practices against workers, and preparing an HR Department to use E-Verify. The training assists employer understanding of how to use E-Verify in a responsible manner without violating prohibitions against discrimination. For more information, contact CRCL at crcltraining@dhs.gov, (202) 357-8258.

Homeland Security Information Network (HSIN) is a user-driven, web-based, sensitive but unclassified (SBU) information sharing platform that connects a broad range of homeland security mission partners. One portal of the

HSIN enterprise is HSIN-CS, managed by the Office of Infrastructure Protection. DHS has designated HSIN-CS to be its primary information-sharing platform between Critical Infrastructure Key Resource sector stakeholders. HSIN-CS enables DHS and critical infrastructure owners and operators to communicate, coordinate, and share sensitive and sector-relevant information to protect their critical assets, systems, functions and networks, at no charge to sector stakeholders. Vetted critical infrastructure private sector owners and operators are eligible to access HSIN-CS. To request access to HSIN-CS, please e-mail CIKRISEAccess@hq.dhs.gov. When requesting access, please indicate the critical infrastructure sector to which your company belongs and include your name, company, official e-mail address, and supervisor's name and phone number. For more information, see www.dhs.gov/hsin or contact hsin.helpdesk@dhs.gov, (866) 430-0162.

Intelligence and Analysis Private Sector Partnership Program The Office of Intelligence and Analysis (I&A) strives to synchronize information sharing of timely, accurate, and actionable intelligence information with the private sector across the spectrum of business and security operations with respect to protecting privacy and civil rights and civil liberties. I&A provides private sector businesses, groups, and trade associations with tailored threat briefings to meet their security information needs. Additionally, the office creates intelligence products that are posted on the Homeland Security Information Network-Critical Sectors (HSIN-CS) portal for use by vetted critical infrastructure owners and operators. For more information, see www.dhs.gov/hsin. To request access to HSIN-CS, e-mail CIKRISEAccess@hq.dhs.gov. When requesting access, please indicate the critical infrastructure sector to which your company belongs and include your name, company, official e-mail address, and supervisor's name and phone number. For more information, contact I&APrivateSectorCoordinator@hq.dhs.gov or call (202) 447-3517 or (202) 870-6087.

Lessons Learned and Information Sharing (LLIS.gov), a US Department of Homeland Security (DHS)/Federal Emergency Management Agency program, is the national online network of lessons learned, best practices, and innovative ideas for the emergency response and homeland security communities. This information and collaboration resource helps emergency response providers and homeland security officials prevent, protect against, respond to, and recover from terrorist attacks, natural disasters, and other emergencies. To register for LLIS, please visit www.llis.gov, contact the program via e-mail feedback@llis.dhs.gov, or call (866) 276-7001.

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 to implement the program. OSDBU makes available forecasts of contract opportunities, vendor outreach sessions, a list of component small business specialists, DHS prime contractors, and information about the DHS mentor-protégé program. See http://www.dhs.gov/openforbusiness or contact OSDBU, (202) 447-5555.

DHS Open Source Enterprise Daily Intelligence Reports provide open source information on several topics of interest. The following are currently available open source reports: **The DHS Daily Digest Report, The DHS Daily Cyber Report, The DHS Daily Infectious Diseases Report, The DHS Daily Human Trafficking and Smuggling Report, The DHS Daily Drug Trafficking and Smuggling Report,** and **The Daily Illicit Commercial Trafficking and Smuggling Report**. These reports may be accessed on the Homeland Security Information Network (HSIN) or private sector partners may request that they be added to distribution by e-mailing OSINTBranchMailbox@hq.dhs.gov with subject line reading "Request DHS Daily [name] Report".

The National Information Exchange Model (NIEM) Program is a Federal, State, local and Tribal interagency initiative providing a national approach and common vocabulary for information exchange. NIEM has a robust training curriculum that is accessible both in classroom and on-line. The primary audience for the NIEM Training Program is Executives, Project and Program Managers, Architects and Technical Implementers within Federal, State, local, Tribal and Private Entities. Additional information on the training courses and NIEM can be obtained by visiting www.NIEM.gov or e-mailing NIEMPMO@NIEM.gov.

Ready Business The U.S. Department of Homeland Security and the Advertising Council launched the *Ready Business* Campaign in September 2004. This extension of the successful *Ready* Campaign, *Ready Business* helps owners and managers of small- and medium-sized businesses prepare their employees, operations and assets in the event of an emergency. For free tools and resources, including how to create a business emergency plan, please visit www.ready.gov.

Traveler Redress Inquiry Program (DHS TRIP) provides a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at airports, train stations, or crossing U.S. borders. To initiate an inquiry, please log onto DHS TRIP's interactive Web site www.dhs.gov/trip. For more information, contact the TSA Contact Center, (866) 289-9673.

U.S. Citizenship and Immigration Services (USCIS)

U.S. Citizenship and Immigration Services (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. www.uscis.gov

USCIS Asylum Program resources include an information guide for prospective asylum applicants available in a number of languages. For more information, visit www.uscis.gov/asylum.

E-Verify is an Internet-based system that allows an employer, using information reported on an employee's Form I-9, to determine the eligibility of that employee to work in the United States. For most employers, the use of E-Verify is voluntary and limited to determining the employment eligibility of new hires only. There is no charge to employers to use E-Verify. Available resources include a demonstration video, fact sheets, weekly webinars, an overview presentation, brochures and posters for employers and employees, and a rights and responsibilities guide. See http://www.dhs.gov/everify. Contact E-Verify@dhs.gov, (888) 464-4218 with any questions or comments.

U.S. Civics and Citizenship Online Resource Center for Instructors provides information about USCIS' Resource Center to help instructors prepare students for naturalization and incorporate civics into ESL instruction. See http://www.uscis.gov/files/nativedocuments/M-662.pdf.

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

Expanding ESL, Civics, and Citizenship Education in Your Community: A Start-Up Guide provides an overview and recommendations to help organizations design and offer ESL and civics/citizenship classes for immigrants. See http://www.uscis.gov/files/nativedocuments/M-677.pdf.

USCIS Genealogy Program is a fee-for-service program providing family historians and other researchers with timely access to historical immigration and naturalization records. The USCIS Genealogy Program offers two services: **Index Search** using biographical information provided by the researcher and a **Record Copy Request** where researchers with valid record citations (USCIS file numbers), gained through a USCIS Genealogy Program index search or through independent research, may request copies of historical immigration and naturalization records. Questions about the USCIS Genealogy Program may be sent to Genealogy.USCIS@dhs.gov. For more information, see http://www.uscis.gov/portal/site/uscis/menuitem.eb1d4c2a3e5b9ac89243c6a7543f6d1a/?vgnextoid=d21f3711ca5ca110VgnVCM1000004718190aRCRD&vgnextchannel=d21f3711ca5ca110VgnVCM1000004718190aRCRD.

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

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.

USCIS Information for Employers and Employees on the employment authorization verification process and the immigration petition process. See http://www.uscis.gov/portal/site/uscis/menuitem.eb1d4c2a3e5b9ac89243c6a7543f6d1a/?vgnextoid=ff1d83453d4a3210VgnVCM100000b92ca60aRCRD&vgnextchannel=ff1d83453d4a3210VgnVCM100000b92ca60aRCRD. For more information contact Public.Engagement@dhs.gov.

USCIS Office of Public Engagement (OPE) seeks to focus on open, candid, and constructive collaboration with community stakeholders at all levels. OPE coordinates and directs USCIS-wide dialogue with external stakeholders to advance the Agency's vision of customer inclusiveness by actively engaging stakeholders to ensure information flow and to institutionalize a mechanism whereby their input will be considered in the process of policy formulation, priority calibration, and assessment of organizational performance. The goal of the office is to provide information and invite feedback to inform our work. See the Outreach tab at http://www.uscis.gov. For more information contact Public.Engagement@dhs.gov.

USCIS Resources USCIS offers a variety of resources for our customers, the organizations that serve them and the public. USCIS is committed to supporting the resource needs of stakeholders, including Congress, community-based organizations and legal practitioners, and educators and researchers. Resources include customer guides, videos, citizenship toolkits, an immigration law glossary, reports and studies, civics and citizenship education resources, and a historical library. See the "Resources" section at http://www.uscis.gov. For more information contact Public.Engagement@dhs.gov.

Welcome to the United States: A Guide for New Immigrants With this landmark publication, the federal government reaches out to new immigrants with essential orientation materials needed to adjust to life in America. It also contains basic history and civics information that introduces new immigrants to U.S. history and the system of government. See http://www.uscis.gov/files/nativedocuments/M-618.pdf.

Citizenship and Immigration Services Ombudsman (CIS Ombudsman)

The CIS Ombudsman is a separate office within the Department of Homeland Security dedicated to improved national security, efficiency, and customer service in the immigration benefits process. The CIS Ombudsman provides recommendations for resolving individual and employer problems with the United States Citizenship and Immigration Services (USCIS). The CIS Ombudsman assists individuals and employers in resolving problems with USCIS; identifies areas in which individuals and employers have problems in dealing with USCIS; and proposes changes to mitigate identified problems. Please note that the CIS Ombudsman is not part of USCIS. The CIS Ombudsman is dedicated to open and accessible communication with both individuals and employers and not only welcomes, but encourages your comments. Comments, examples, and suggestions may be sent to the Ombudsman at cisombudsman@dhs.gov. www.dhs.gov/cisombudsman

CIS Ombudsman Annual Reports to Congress By June 30 of each calendar year, the Annual Report is delivered to the House and Senate Committees on the Judiciary without any prior comment or amendment from any administrative agency official including: the Secretary, Deputy Secretary, or Director of USCIS. The Ombudsman's annual reports focus on identifying systemic issues that cause delay in granting immigration benefits as well as pervasive and serious problems faced by individuals and employers in their interactions with USCIS. The Annual Report contains cumulative analysis and recommendations and provides details on activities undertaken by the Ombudsman during the reporting period of June 1 through May 31 of the calendar year. See http://www.dhs.gov/xabout/structure/gc_1183996985695.shtm.

CIS Ombudsman's Community Call-In Teleconference Series provides an opportunity to discuss your interactions with U.S. Citizenship and Immigration Services (USCIS) and share your comments, thoughts, and suggestions as well as any issues of concern. For more information, including questions and answers from previous teleconference and a schedule of upcoming calls, visit http://www.dhs.gov/xabout/structure/gc_1171038701035.shtm. To participate in these calls, please RSVP to cisombudsman.publicaffairs@dhs.gov specifying which call you would like to join. Participants will receive a return e-mail with the call-in information.

CIS Ombudsman Updates share information on current trends and issues to assist individuals and employers in resolving problems with USCIS. See http://www.dhs.gov/xabout/structure/gc_1221837986181.shtm.

Previous Recommendations by the CIS Ombudsman are intended to ensure national security and the integrity of the legal immigration system, increase efficiencies in administering citizenship and immigration services, and improve customer service in the rendering of citizenship and immigration services. Problems reported to the Ombudsman by individuals and employers (during the Ombudsman's travels), discussions with immigration stakeholders, and suggestions of USCIS employees themselves provide the basis for many of the recommendations. To view the recommendations as well as USCIS responses, see http://www.dhs.gov/files/programs/editorial_0769.shtm.

Send Your Recommendations to the CIS Ombudsman Your recommendations are accepted and encouraged. The Ombudsman is dedicated to identifying systemic problems in the immigration benefits process and preparing recommendations for submission to U.S. Citizenship and Immigration Services (USCIS) for process changes. The Ombudsman believes that process change recommendations from individuals like you represent one of the best sources for identifying systemic problems in the immigration benefits process. Ideally, your recommendations for process changes should not only identify the problem you are experiencing, but should also contain a proposed solution that will not only benefit your individual case, but others who may be experiencing the same problem as well. Send your comments, examples, and suggestions to cisombudsman@dhs.gov or to the following mailing address:

Citizenship and Immigration Services Ombudsman
ATTN: Recommendations
United States Department of Homeland Security
Mail Stop 1225
Washington, D.C. 20528-1225

Submit a Case Problems to the CIS Ombudsman If you are experiencing problems during the adjudication of an immigration benefit with U.S. Citizenship and Immigration Services (USCIS), you can submit a case problem to the CIS Ombudsman using DHS Form 7001 (CIS Ombudsman Case Problem Submission Form). To submit a case problem 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 Case Problem using DHS Form 7001: Section 15 Consent). See http://www.dhs.gov/files/programs/editorial_0497.shtm.

U.S. Coast Guard (USCG)

For over two centuries the U.S. Coast Guard has safeguarded our Nation's maritime interests in the heartland, in the ports, at sea, and around the globe. We protect the maritime economy and the environment, we defend our maritime borders, and we save those in peril. This history has forged our character and purpose as America's Maritime Guardian — *Always Ready* for all hazards and all threats. www.uscg.mil

America's Waterways Watch is a combined effort of the U.S. Coast Guard 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 visit http://www.americaswaterwaywatch.us. To report suspicious activity call 877-24WATCH (877-249-2824).

U.S. Coast Guard Auxiliary is the uniformed volunteer component of the United States Coast Guard. Created by an Act of Congress in 1939, the Auxiliary directly supports the Coast Guard in all missions, except military and law enforcement actions. The Auxiliary conducts safety patrols on local waterways, assist the Coast Guard with homeland security duties, teach boating safety classes, conduct free vessel safety checks for the public, as well as many other activities. The Auxiliary has members in all 50 states, Puerto Rico, the Virgin Islands, American Samoa and Guam. For more information, visit http://www.cgaux.org/.

U.S. Coast Guard Maritime Information eXchange ("CGMIX") makes U.S. Coast Guard (USCG) maritime information available on the public 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. See http://cgmix.uscg.mil/.

U.S. Coast Guard Navigation Center provides services for safe, secure, and efficient maritime transportation by delivering: enhanced situational awareness through continuous monitoring and managing of vessel movement system, quality positioning, navigation and timing signals, accurate and timely maritime information services, and system requirements and performing operational oversight of premier navigation services. See http://www.navcen.uscg.gov/. For more information use the e-mail Inquiry located at http://www.navcen.uscg.gov/misc/NIS_contact_us.htm or call (703) 313-5900.

HOMEPORT is an internet repository of detailed information of interest to the Port Community. Specific Homeport Topics Include: Containers, Domestic Vessels (US Flag Vessels), Environmental, Facilities, Incident Management and Preparedness, Investigations (Maritime Casualties and Incidents), Marine Safety, Maritime Domain Awareness (MDA) & Information Sharing (IS), Maritime Security, Merchant Mariners, Port State Control, Ports and Waterways, Regulations/Administrative Adjudications, Strategic Initiatives, USCG Sector (Field Unit) Directory, Vessel Standards, Counter Piracy, International Port Security (IPS) Program, Maritime Transportation Security Act (MTSA), Marine Safety Center, Mariner Credential Verification, and Mariner Credential Application Status. See http://homeport.uscg.mil.

USCG National Maritime Center (NMC) issues Merchant Mariner Credentials (MMC) to fully qualified US mariners, approves and audits training programs and courses offered by mariner training organizations throughout the United States, and provides information about merchant mariner records. For more information, see http://www.uscg.mil/nmc or contact NMC Customer Service Center**:** (888) IASKNMC (1-888-427-5662).

National Vessel Movement Center (NVMC) provides the maritime industry with a method to submit electronically a Notice of Arrival and a Notice of Departure, which fulfills USCG and the Customs and Border Protection's (CBP) requirements. See http://www.nvmc.uscg.gov or contact the NVMC sans@nvmc.uscg.gov, (800) 708-9823 or (304) 264-2502.

Vessel Documentation (for US Flag Vessels) The National Vessel Documentation Center facilitates maritime commerce and the availability of financing while protecting economic privileges of United States citizens through the enforcement of regulations, and provides a register of vessels available in time of war or emergency to defend and protect the United States of America. See http://www.uscg.mil/hq/cg5/nvdc/. For more information call (800) 799-8362 or (304) 271-2400 (7:30 a.m. to 5:00 p.m. Eastern Time).

U.S. Customs and Border Protection (CBP)

CBP is one of the Department of Homeland Security's largest and most complex components, with a priority mission of keeping terrorists and their weapons out of the U.S. It also has a responsibility for securing and facilitating trade and travel while enforcing hundreds of U.S. regulations, including immigration and drug laws. www.cbp.gov

CBP Publications and Guidance

AIRBUST program provides awareness of suspicious small aircraft and behaviors. The AIRBUST Card is a pocket-sized laminated card displaying the phone number that people can call to report suspicious or low flying aircraft, 1-866-AIRBUST (1-866-247-2878). This number rings directly to the CBP Air and Marine Operations Center (AMOC) Floor and anyone can use the phone number for reporting. On one side of the card are drawings of single- and twin-engine aircraft often used to transport contraband. The opposite side of the card lists helpful information to note when reporting. The AIRBUST poster, CBP Publication 0000-0716, is an 8.5x11 poster with the 1-866-AIRBUST (1-866-247-2878) phone number. It also lists four general items of interest that can tip off a general aviation airport employee or law enforcement official that a particular aircraft or pilot may be involved in illicit activity. For more information, or to order these publications, call 951-656-8000.

CBP Directives Pertaining to Intellectual Property Rights are policy guidance documents that explain CBP's 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, please visit http://www.cbp.gov/xp/cgov/trade/legal/directives/. For additional information, or e-mail CBP IPR Policy and Programs at iprpolicyprograms@dhs.gov.

Entry Level Test Study Guides for CBP Job Applicants CBP provides study guides and test preparation materials for applicants to several core occupations. Applicants for Border Patrol Agent, Customs and Border Protection Officer & Agriculture Specialist, and Intelligence Research Specialist positions will find these resources beneficial during their application process. These resources provide test taking hints, helpful information on how to prepare for a test, and practice tests. For more information, please visit: http://cbp.gov/xp/cgov/careers/study_guides/.

Intellectual Property Rights (IPR) Seizure Statistics CBP maintains statistics on IPR seizures made by the Department of Homeland Security (CBP and ICE) at: http://www.cbp.gov/xp/cgov/trade/priority_trade/ipr/pubs/seizure/. For any specific questions or concerns, please contact CBP by e-mail at: iprpolicyprograms@dhs.gov or ipr.helpdesk@dhs.gov.

U.S. Border Patrol Checkpoints Brochure provides information for the public about Border Patrol checkpoints available at: http://www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/border/border_patrol/bp_checkpoints.ctt/bp_checkpoints.pdf.

CBP Alerts and Newsletters

Informed Compliance Publications are available on a specific trade issue, which summarizes practical information for the trade community to better understand their obligations under Customs and related laws. These publications are available at: http://www.cbp.gov/xp/cgov/trade/legal/.

U.S. Border Patrol Blotter, Newsletter, and Alerts compiles the latest information on noteworthy occurrences documenting apprehensions of criminals, seizures of illegal drugs, rescue missions, and many other Border Patrol success stories from around the country. These highlights can be found at: http://cbp.gov/xp/cgov/border_security/border_patrol/weekly_blotter/. The border patrol also publishes a newsletter: http://www.cbp.gov/xp/cgov/newsroom/publications/frontline_magazine/ and alerts: http://www.cbp.gov/xp/cgov/newsroom/advisories/.

CBP Technical Assistance

1-800 BE ALERT The public is welcome to actively participate in helping to secure our nation's borders by reporting suspicious activity to the U.S. Border Patrol via a toll free telephone reporting system: "BE ALERT". To report suspicious activity: Call (800) BE ALERT or (800) 232-5378. For more information on U.S. Border Patrol Checkpoints: Call (877) 227-5511. International Callers Call +1 (703) 526-4200.

Automated Commercial Environment (ACE) National Help Desk provides customer technical support services 24 hours a day, seven days a week, including information about ACE Secure Data Portal account access, account management, and report generation. The ACE Help Desk is the first point of contact for all ACE users experiencing system difficulties. To reach the ACE Help Desk, please call: (800) 927-8729.

Cargo Systems Messaging Service (CSMS) is an active, live, searchable database of messages that are of interest to Automatic Broker Interface (ABI) filers, Automated Commercial Environment (ACE) event participants, ACE Portal Accounts users, ACE reports users, air carriers, ocean carriers, Periodic Monthly Statement participants, and rail and truck carriers. CSMS is augmented by an e-mail subscription service, which is available at: https://service.govdelivery.com/service/multi_subscribe.html?code=USDHSCBP&custom_id=938&origin=https://apps.cbp.gov/csms.

CBP Client Representatives are the first points of contact for importers, exporters, transportation providers, and brokers wishing to automate any of their Customs processes. Client Representatives are the contact point for all system-related problems and questions from trade partners. For more information about client reps and the services offered to members of the trade, please visit:

http://www.cbp.gov/xp/cgov/trade/automated/automated_systems/client_reps.xml or contact the CBP Client Representative Office at: (571) 468-5000.

CBP INFO Center Self Service Q&A Database is a searchable database with over 600 answers to commonly (and not so commonly) asked questions about CBP programs, requirements, and procedures. If visitors to the site are unable to find an answer to their question, they may also submit an inquiry or complaint for personal assistance. To use the searchable database, please visit https://help.cbp.gov/cgi-bin/customs.cfg/php/enduser/home.php?p_sid=YeyXThOj. Or call the CBP INFO Center at (877) CBP-5511 or (703) 526-4200.

Entry Process into United States CBP welcomes more than 1.1 million international travelers into the United States at land, air, and seaports on an average day. U.S. citizens and international visitors should consult the following publications and factsheets for information to simplify their entry into the United States. For information about international travel, visit http://www.cbp.gov/xp/cgov/travel/. For more information, please contact the CBP Information Center at (877) 227-5511.

Importing into the United States CBP will facilitate about $2 trillion in legitimate trade this year while enforcing U.S. trade laws that protect the economy and the health and safety of the American people. We accomplish this through close partnerships with the trade community, other government agencies, and foreign governments. See http://www.cbp.gov/linkhandler/cgov/newsroom/publications/trade/iius.ctt/iius.pdf. For information about CBP Trade programs, visit http://www.cbp.gov/xp/cgov/trade/.

CBP Programs and services

Automated Commercial Environment (ACE) is the United States' commercial trade processing system designed to automate border processing, to enhance border security, and to foster our Nation's economic security through lawful international trade and travel. ACE will eventually replace the current import processing system for CBP, the Automated Commercial System (ACS). ACE is part of a multi-year CBP modernization effort and is being deployed in phases. For more information about ACE, please visit http://www.cbp.gov/xp/cgov/trade/automated/modernization/.

Automated Commercial System (ACS) is a data information system used by CBP to track, control, and process commercial goods imported into the United States. Through the use of Electronic Data Interchange (EDI), ACS facilitates merchandise processing for CBP and the private sector. ACS is accessed through the CBP Automated Broker Interface (ABI) and permits qualified participants to electronically file required import data with CBP. ABI is a voluntary program available to brokers, importers, carriers, port authorities, and independent service centers. For more information about ACS, please visit http://www.cbp.gov/xp/cgov/trade/automated/automated_systems/acs/. For additional information specific to ABI, please contact the CBP Client Representative Office at (571) 468-5000.

Automated Export System (AES) is the electronic way to file export declarations and ocean manifest information with CBP. For more information about AES, including technical documentation, software vendors, and other items of interest, please visit http://www.cbp.gov/xp/cgov/trade/automated/aes/.

Automated Manifest System (AMS) is a multi-modular cargo inventory control and release notification system. AMS facilitates the movement and delivery of cargo by multiple modes of transportation. Carriers, port authorities, service bureaus, freight forwarders, and container freight stations can participate in AMS. Sea AMS allows participants to transmit manifest data electronically prior to vessel arrival. CBP can then determine in advance whether the merchandise merits examination or immediate release. Air AMS allows carriers to obtain notifications of releases, in-bond authorizations, general order, permit to proceed, and local transfer authorization upon flight departure or arrival from the last foreign port. Rail AMS allows rail carriers to electronically transmit information to CBP. When all bills on a train are assigned, the rail carrier transmits a list of the bills and containers in standing car order. For more information about AMS, please visit http://www.cbp.gov/xp/cgov/trade/automated/automated_systems/acs/acs_ams.xmlACS.

Carrier Liaison Program (CLP) This 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 CLP, please visit http://www.cbp.gov/xp/cgov/travel/inspections_carriers_facilities/clp/, e-mail CLP@dhs.gov, or call (202) 344-3440.

Customs-Trade Partnership Against Terrorism (C-TPAT) is a voluntary government-business initiative to strengthen and improve the overall international supply chain and U.S. border security. C-TPAT recognizes that CBP can provide the highest level of cargo security only through close cooperation with the ultimate owners of the international supply chain such as importers, carriers, consolidators, licensed customs brokers, and manufacturers. Through this initiative, CBP is asking businesses to ensure the integrity of their security practices, communicate, and verify the security guidelines of their business partners within the supply chain. For more information, or to apply online, please visit http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/. For questions or concerns, please contact the CBP Industry Partnership Program at (202) 344-1180, or by fax (202) 344-2626 or e-mail, industry.partnership@dhs.gov.

eAllegations provides concerned members of the public a means to confidentially report suspected trade violations to CBP. For more information, or to initiate an investigation, please visit https://apps.cbp.gov/eallegations/, or contact the Commercial Targeting and Enforcement, Office of International Trade at: (800) BE-ALERT.

Electronic System for Travel Authorization (ESTA) is a free, automated system that determines the eligibility of visitors to travel to the U.S. under the Visa Waiver Program. The ESTA application collects the same information collected on Form I-94W. ESTA applications may be submitted at any time prior to travel, though it is recommended travelers apply when they begin preparing travel plans. To apply online, please visit:

https://esta.cbp.dhs.gov/. For additional information, please call: (202) 344-3710.

Global Entry is a pilot program managed by CBP, which allows pre-approved, low-risk travelers, expedited clearance upon arrival into the United States. Although this program is intended for "frequent travelers" who make several international trips per year, there is no minimum number of trips an applicant must make in order to qualify. For more information about Global Entry, please visit: http://www.cbp.gov/xp/cgov/travel/trusted_traveler/global_entry/ or apply online at: https://goes-app.cbp.dhs.gov/. For additional questions or concerns, please contact CBP by e-mail, cbp.goes.support@dhs.gov, or by phone, (866) 530-4172.

Importer Self-Assessment Program (ISA) is a voluntary approach to trade compliance. The program provides the opportunity for importers to assume responsibility for monitoring their own compliance in exchange for benefits. Public information regarding this program, including frequently asked questions, policy information, best practices, and requirements can be found at http://www.cbp.gov/xp/cgov/trade/trade_programs/importer_self_assessment/.

Importer Self Assessment – Product Safety Pilot (ISA-PS) CBP and the Consumer Product Safety Commission (CPSC) have a strong history of partnership in combating unsafe imports and have worked together on significant product recalls. CBP announces a new partnership with CPSC and importers to prevent unsafe imports from entering the United States. For more information, please visit http://www.cbp.gov/xp/cgov/trade/trade_programs/importer_self_assessment/isa_safety_pilot.xml.

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, please visit http://www.cbp.gov/xp/cgov/trade/priority_trade/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. CBP's 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 please visit: http://iprs.cbp.gov/. For additionalinformation, please e-mail at hqiprbranch@dhs.gov or call (202) 325-0020.

Intellectual Property Rights (IPR) Continuous Sample Bond CBP established a new 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. A sample bond template can be downloaded at: http://www.cbp.gov/xp/cgov/trade/trade_programs/bonds/ipr_bonds_samples/. For additional information, please contact CBP's Revenue Division, Office of Finance by e-mail at: cbp.bondquestions@dhs.gov, or by phone at (317) 614-4880 or by fax at (317) 614-4517.

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. To reach the CBP IPR Help Desk, please call at (562) 980-3119 ext. 252, or e-mail at ipr.helpdesk@dhs.gov.

Intellectual Property Rights (IPR) and Restricted Merchandise Branch oversees the IPR recordation program and provides IPR infringement determinations and rulings. For legal questions about CBP's IPR recordation program, please e-mail at: hqiprbranch@dhs.gov, or call (202) 325-0020.

Intellectual Property Rights (IPR) U.S. – EU Joint Brochure and Web Toolkit for Trademark, Copyright Owners To promote strong and effective border enforcement of Intellectual Property Rights, CBP and Customs Officials in the European Union have jointly developed a brochure and Web toolkit to assist intellectual property owners in working with Customs to enforce their rights and to prepare information to help U.S. and E.U. Customs Agencies determine whether goods are counterfeit or pirated. To access the Protecting Intellectual Property Rights at Our Borders brochure, please visit: http://www.cbp.gov/linkhandler/cgov/trade/priority_trade/ipr/pubs/cpg_final_090306.ctt/cpg_final_090306.pdf. To access the Toolkit, please visit: http://www.cbp.gov/linkhandler/cgov/trade/priority_trade/ipr/cpg_final_090306.ctt/cpg_final_090306.pdf. For additional questions or concerns, please contact the IPR Help Desk by e-mail, ipr.helpdesk@dhs.gov or phone, (562) 980-3119 ext. 252.

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

National Gang Intelligence Center is a multi-agency effort that integrates the gang intelligence assets of Federal, State, and local law enforcement entities to serve as a centralized intelligence resource for gang information and analytical support. The mission of the NGIC is to support law enforcement agencies through timely and accurate information sharing and strategic/tactical analysis of Federal, State, and Local law enforcement intelligence focusing on the growth, migration, criminal activity, and association of gangs that pose a significant threat to communities throughout the United States. The NGIC concentrates on gangs operating on a national level that demonstrate criminal connectivity between sets and common identifiers and goals. Because many violent gangs do not operate on a national level, the NGIC will also focus on regional-level gangs. The NGIC produces intelligence assessments, intelligence bulletins, joint agency intelligence products, and other non-standard intelligence products for our customers. For more information, please contact the NGIC, (703) 414-8600.

Private Aircraft Travel Entry Programs The *Advance Information on Private Aircraft Arriving and Departing the United States* final rule requires that pilots of private aircraft submit advance notice and manifest data on all persons traveling on board. Required information must be submitted to CBP via an approved electronic data interchange system no later than 60 minutes prior to departure. The CBP.gov web site offers information about current CBP policies, regulations, documentary requirements, and ports of entry. For more information, please visit http://www.cbp.gov/xp/cgov/travel/inspections_carriers_facilities/apis/. For additional questions or concerns, please contact CBP via e-mail at Private.Aircraft.Support@dhs.gov.

Secure Freight Initiative (SFI) and Importer Security Filing and additional carrier requirements (10+2) The Secure Freight Initiative (SFI), through partnerships with foreign governments, terminal operators, and carriers enhances DHS's capability to better assess the security of U.S.-bound maritime containers by scanning them for nuclear and other radioactive materials before they are laden on vessels bound for the United States. For the domestic CBP officers, SFI provides additional data points that are used in conjunction with advanced data, such as 24-hour rule information, 10+2, Customs-Trade Partnership Against Terrorism information, and the Automated Targeting System to assess the risk of each container coming to the United States. For more information, please visit http://www.cbp.gov/xp/cgov/trade/cargo_security/secure_freight_initiative/, or e-mail questions to securefreightinitiative@dhs.gov.

CBP Trade Outreach The Office of Trade Relations supports communications between CBP and the private sector, and provides information for new importers, exporters and small businesses. For more information, please visit http://www.cbp.gov/xp/cgov/trade/trade_outreach/.

Trusted Traveler Programs (TTP) include FAST-Driver, NEXUS, SENTRI, and Global Entry. TTP provide expedited travel for pre-approved, low risk travelers through dedicated lanes and kiosks (NEXUS at Canadian Pre-Clearance ports). Program members received RFID embedded cards that facilitate border processing by confirming membership, identity, and running law enforcement checks. For more information about a CBP's trusted traveler programs, please visit http://www.cbp.gov/xp/cgov/travel/trusted_traveler/.

Visa Waiver Program (VWP) enables citizens and nationals from 34 countries to travel to and enter the United States for business or visitor purposes for up to 90 days without obtaining a visa. For more information about the Visa Waiver Program, please visit http://www.cbp.gov/xp/cgov/travel/id_visa/business_pleasure/vwp/.

Western Hemisphere Travel Initiative (WHTI) requires all travelers, U.S. citizens and foreign nationals, to present a passport or other acceptable documents that denote identity and citizenship when entering the United States. For more information about WHTI, please visit: http://www.getyouhome.gov/, or contact CBP Customer Service at (877)227-5511 or (703) 526-4200, TDD: (866) 880-6582.

Cybersecurity and Communications (CS&C)

The Office of Cybersecurity and Communications (CS&C) is responsible for enhancing the security, resiliency, and reliability of the nation's cyber and communications infrastructure. CS&C actively engages the public and private sectors as well as international partners to prepare for, prevent, and respond to catastrophic incidents that could degrade or overwhelm these strategic assets. http://www.dhs.gov/xabout/structure/gc_1185202475883.shtm

CS&C Training and Education

Control Systems Security Program (CSSP) Instructor-Lead Cybersecurity Trainingis provided through an introductory course for IT professionals or a 5-day advanced course which includes hands-on instruction in an actual control system environment. For more information, see http://www.us-cert.gov/control_systems/cstraining.html, or contact CSSP@dhs.gov.

Cyber Education and Workforce Development Program (CEWD) As cyber threats and their sophistication increase, the demand for qualified IT security professionals increases as well. In response, the National Cyber Security Division's Cyber Education and Workforce Development program (CEWD) developed the IT Security Essential Body of Knowledge (EBK). The IT Security EBK is an umbrella framework that links competencies and functional perspectives to IT security roles to accurately reflect a national perspective. See http://www.us-cert.gov/ITSecurityEBK/.

CS&C Publications and Guidance

Cybersecurity Information Products and Recommended Practices provide current cybersecurity information resources and recommend security practices to help industry understand emerging control systems cyber security issues and mitigate vulnerabilities. This information will help 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. An interactive site with recommended practices for control system networks can be found at http://csrp.inl.gov/. For more information, contact CSSP@dhs.gov.

Cybersecurity Public Trends and Analysis Report provides awareness of the cyber security 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. Contact US-CERT at info@us-cert.gov, (888) 282-0870

Cyber Security Evaluation Tool (CSET) is a desktop software tool that guides users through a step-by-step process for assessing the cyber security posture of their industrial control system and enterprise information technology networks. CSET is available in DVD format. To learn more, visit http://www.us-cert.gov/control_systems/satool.html. To obtain a DVD copy of CSET, send an e-mail with your mailing address to CSET@dhs.gov.

Emergency Communications Guidance Documents and Methodologies The DHS Office of Emergency Communications develops 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 on improving statewide governance, developing standard operating procedures, managing technology, supporting training and exercises, and encouraging usage of interoperable communications, among other topics. Each is available publicly and is updated as needed. Examples include: *Establishing Governance to Achieve Statewide Communications Interoperability* and the *Formal Agreement and Standard Operating Procedure Template Suite.* For more information, contact the Office of Emergency Communications at oec@hq.dhs.gov or visit http://www.safecomprogram.gov.

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

Information Technology Sector Risk Assessment (ITSRA) The National Cyber Security Division (NCSD), in partnership with public and private sector partners from the IT Sector Coordinating Council (IT SCC) and the IT Government Coordinating Council (IT GCC), released the baseline ITSRA in 2009. The ITSRA provides an all-hazards risk profile that public and private IT Sector partners can use to inform resource allocation for research and development and other protective measures which enhance the security and resiliency of the critical IT Sector functions. By increasing the awareness of risks across the public and private sectors, the Baseline Risk Assessment is the foundation for ongoing national-level collaboration to enhance the security and resiliency of the critical IT Sector functions. See http://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf. For more information, contact ncsd_cipcs@hq.dhs.gov.

Information Technology Sector Specific Plan (IT SSP) the National Cyber Security Division (NCSD), in partnership with private sector members of the IT Sector, has developed the IT SSP to outline the IT Sector security partners' joint implementation of the NIPP risk management framework. It describes an approach for identifying, assessing, prioritizing, and protecting critical IT Sector functions, establishing shared IT Sector goals and objectives, and aligning initiatives to meet them. To view the IT SSP, visit

http://www.dhs.gov/xlibrary/assets/IT_SSP_5_21_07.pdf. For more information, contact ncsd_cipcs@hq.dhs.gov.

National Emergency Communications Plan (NECP) is a strategic plan that sets goals and identifies key national priorities to enhance governance, planning, technology, training and exercises, and disaster communications capabilities. The NECP establishes specific national priorities to help State and local jurisdictions improve communications interoperability by adopting a series of goals and milestones that measure interoperability achievements over a period of years beginning in 2008, and ending in 2013. In order to successfully implement the NECP, increased collaboration between the public and private sector will be needed. As a result, the plan establishes specific initiatives and milestones to increase such collaboration. For more information, see http://www.dhs.gov/xlibrary/assets/national_emergency_communications_plan.pdf or contact the Office of Emergency Communications, oec@hq.dhs.gov.

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

SAFECOM Guidance for Federal Grant Programs The Department of Homeland Security Office of Emergency Communications, in coordination with the Office for Interoperability and Compatibility, develops the annual *SAFECOM Guidance for Federal Grant Programs*. Although SAFECOM is not a grant-making body, the guidance outlines recommended allowable costs and applications requirements for Federal grant programs providing funding for interoperable emergency communications. The guidance is intended to ensure that Federal grant funding for interoperable communications aligns with national goals and objectives and ensures alignment of State, local, and tribal investment of Federal grant funding to statewide and national goals and objectives. See http://www.safecomprogram.gov/NR/rdonlyres/31A870C0-0C9D-4C29-86F8-147D61AF25CF/0/FY_2010_SAFECOM_Recommended_Guidance__111809__Final.pdf. For more information, contact the Office of Emergency Communications at oec@hq.dhs.gov.

U.S. Computer Emergency Readiness Team (US-CERT) Monthly Activity Summary summarizes general activity as well as updates made to the National Cyber Alert System each month. This includes current activity updates, technical and non-technical alerts, bulletins, and tips, in addition to other newsworthy events or highlights. See http://www.us-cert.gov/reading_room/index.html#news, contact US-CERT at info@us-cert.gov, (888) 282-0870.

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

U.S. Computer Emergency Readiness Team (US-CERT) Vulnerability Notes Databaseincludes technical descriptions of the vulnerability, as well as the impact, solutions and workarounds, and lists of affected vendors. See http://www.kb.cert.org/vuls, contact US-CERT at info@us-cert.gov, (888) 282-0870.

CS&C Alerts and Newsletters

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

Critical Infrastructure Information Notices are intended to provide warning to critical infrastructure owners and operators when a particular cyber event or activity has the potential to impact critical infrastructure computing networks. This document is distributed only to those parties who have a valid "need to know," *a direct role in securing networks or systems that enable or support U.S. critical infrastructures*. Access is limited to a secure portal (https://portal.us-cert.gov) and controlled distribution list. For more information, contact the US-CERT Secure Operations Center at soc@us-cert.gov; (888) 282-0870.

National Cyber Alert System offers a variety of information for users with varied technical expertise including Technical Cybersecurity Alerts and Bulletins or more general-interest pieces such as Cybersecurity Alerts and Tips on a variety of cyber-related topics. See http://www.uscert.gov/cas/alldocs.html. Contact US-CERT at info@us-cert.gov, (888) 282-0870.

CS&C Technical Assistance

U. S. Computer Emergency Readiness Team (US-CERT) Operations Center Report cybersecurity incidents (including unexplained network failures), the discovery of malicious code, and vulnerability information at https://forms.us-cert.gov/report/. Contact the US-CERT Operations Center at soc@us-cert.gov; (888) 282-0870.

Cyber Resiliency Review (CRR) is an assessment offered by the Cyber Security Evaluation Program to measure and enhance the implementation of key cybersecurity capacities and capabilities of critical infrastructure and key resources (CIKR). The purpose of the CRR is to gather information regarding cybersecurity performance from specific CIKR in order to gain an understanding of the relationships and impacts of CIKR performance in protecting critical infrastructure operations. The CRR serves as a repeatable cyber review, while allowing for an evaluation of enterprise-specific cybersecurity capabilities. 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.

Cyber Security Advisors (CSAs) act as principal field liaisons in cybersecurity and provide a Federal resource to regions, communities, and businesses. Their primary goal is to assist in the protection of cyber components essential within the Nation's critical infrastructure and key resources (CIKR). Equally important is their role in supporting cybersecurity risk management efforts at the State and local homeland security initiatives. CSAs will work with established programs in State and local areas, such as Protective Security Advisors, FEMA emergency management personnel, and fusion center personnel. For more information, contact the program at CSE@dhs.gov.

Cyber Security Evaluation Program (CSEP) conducts voluntary cybersecurity assessments across all 18 CIKR Sectors, within state governments, and for large urban areas. CSEP affords CIKR sector participants a portfolio of assessment tools, techniques, and analytics, ranging from those that can be self-applied to those that require expert facilitation or mentoring outreach. The CSEP, in alignment with the DHS National Infrastructure Protection Plan (NIPP), works closely with and coordinates efforts with internal and external stakeholders to measure key performances in cybersecurity management. The Cyber Resiliency Review is being deployed across all 18 Critical Infrastructure Sectors (as denoted by DHS), state, local, tribal, and territorial governments. For more information, visit www.dhs.gov/xabout/structure/editorial_0839.shtm or contact the program at CSE@dhs.gov.

Cybersecurity Vulnerability Assessments through the Control Systems Security Program (CSSP) provide on-site support to critical infrastructure asset owners by assisting them to perform a security self-assessment of their enterprise and control system networks against industry accepted standards, policies, and procedures. To request on-site assistance, asset owners may e-mail CSSP@dhs.gov.

Industrial Control Systems Technology Assessments provide a testing environment to conduct baseline security assessments on industrial control systems, network architectures, software, and control system components. These assessments include testing for common vulnerabilities and conducting vulnerability mitigation analysis to verify the effectiveness of applied security measures. To learn more about ICS testing capabilities and opportunities, e-mail CSSP@dhs.gov.

CS&C Programs and Services

Control Systems Security Program (CSSP) reduces industrial control system risks within and across all critical infrastructure and key resource sectors. CSSP coordinates cybersecurity efforts among Federal, State, local, and Tribal governments, as well as industrial control system owners, operators, and vendors. CSSP provides many products and services that assist the industrial control system stakeholder community to improve their cybersecurity posture and implement risk mitigation strategies. To learn more about the CSSP, visit http://www.us-cert.gov/control_systems/ or e-mail CSSP@dhs.gov.

Critical Infrastructure Protection – Cyber Security (CIP-CS) leads efforts with public and private sector partners to promote an assured and resilient U.S. cyber infrastructure. Major elements of the CIP-CS program include: managing and strengthening cyber critical infrastructure partnerships with public and private entities in order to effectively implement risk management and cybersecurity strategies, teaming with cyber critical infrastructure partners in the successful implementation of cybersecurity strategies, and promoting effective cyber communications processes with partners that result in a collaborative, coordinated approach to cyber awareness. For more information, contact CIP-CS at cip_cs@dhs.gov.

Global Supply Chain Risk Management (GSCRM) Program provides recommendations to standardize and implement risk management processes for acquiring information and communications technologies (ICT) for the federal government, and processes to reduce the threat of attacks to federal ICT through the supply chain. Your organization can help with this initiative by applying sound security procedures and executing due diligence to provide integrity and assurance through the vendor supply chain. For more information, visit http://www.dhs.gov/files/programs/gc_1234200709381.shtm or contact the Global Supply Chain Program at Kurt.Seidling@hq.dhs.gov.

National Vulnerability Database (NVD) is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security-related software flaws, misconfigurations, product names, and impact metrics. For more information, visit http://nvd.nist.gov/ or contact nvd@nist.gov.

SAFECOM Program is a communications program which provides research, development, testing, and evaluation, guidance, tools, and templates on interoperable communications-related issues to local, Tribal, State, and Federal emergency response agencies. The SAFECOM web site provides members of the emergency response community and other constituents with information and resources to help them meet their communications and interoperability needs. The site offers comprehensive information on topics relevant to emergency response communications and features best practices that have evolved from real-world situations. See http://www.safecomprogram.gov, contact SAFECOM@dhs.gov.

Software Assurance Program Software Assurance (SwA) is the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions in the intended manner. Grounded in the National Strategy to Secure Cyberspace, the Department of Homeland Security's Software Assurance Program spearheads the development of practical guidance and tools and promotes research and development of secure software engineering, examining a range of development issues from new methods that avoid basic programming errors to enterprise systems that remain secure when portions of the system software are compromised. Resources including articles, webinars, podcasts, and tools can be found at the SwA Community Resources and Information Clearinghouse located at https://buildsecurityin.us-cert.gov/swa/. For more information, contact software.assurance@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. www.fema.gov

FEMA Training and Education

Are You Ready? An In-depth Guide to Citizen Preparedness provides a step-by-step approach to disaster preparedness by walking the reader through how to get informed about local emergency plans, how to identify hazards that affect their local area, and how to develop and maintain an emergency communications plan and disaster supplies kits. Other topics include what to do before, during, and after each hazard type, including Natural Hazards, Hazardous Materials Incidents, Household Chemical Emergencies, Nuclear Power Plant, and Terrorism (including Explosion, Biological, Chemical, Nuclear, and Radiological hazards). For more information visit www.fema.gov/areyouready or call (800) 480-2520 to order materials**.** Questions regarding the Citizen Corps program can be directed to citizencorps@dhs.gov.

Center for Domestic Preparedness (CDP) offers several programs that are designed for people that have emergency response and healthcare responsibilities, or meet the criteria specified in the web site cited below. CDP offers courses in Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) incident response, toxic agent training, healthcare response for mass casualty incidents, Radiological Emergency Preparedness (REP) Program courses, Field Force Operations, and the National Incident Management System (NIMS). CDP offers integrated training that includes the opportunity to train in the only live agent training facility dedicated to the civilian response community. CDP's healthcare courses include exercises in a training hospital dedicated solely to preparedness and response. CDP offers residential training at its Anniston, Alabama facility and off-campus training throughout the United States. CDP has an integrated training approach that is free of charge to state, local and tribal agencies. Individuals from Federal, International agencies and the private sector are encouraged to attend but, however, must pay a tuition fee for the courses in addition to their own transportation and lodging fees. For more information, see http://cdp.dhs.gov/index.html or call (866) 213-9553.

Community Emergency Response Team (CERT) This program helps train people to be better prepared to respond to emergency situations in their communities. It is a resource for the private sector to use to ensure its employees are prepared for all hazards. When emergencies happen, CERT members can give critical support to first responders, provide immediate assistance to survivors, and organize spontaneous volunteers at a disaster site. CERT members can also help with non-emergency projects that help improve the safety of the community. For more information visit www.citizencorps.gov/cert or contact cert@dhs.gov.

FEMA Emergency Management Institute Independent Study Program The Emergency Management Institute (EMI) offers self-paced courses designed for people who have emergency management responsibilities and for the general public. FEMA's Independent Study Program offers courses that support the nine mission areas identified by the National Preparedness Goal: Incident Management, Operational Planning, Disaster Logistics, Emergency Communications, Service to Disaster Victims, Continuity Programs, Public Disaster Communications, Integrated Preparedness and Hazard Mitigation. For more information on EMI's training courses, please visit http://training.fema.gov/IS/ or contact us (301) 447-1200.

FEMA Emergency Management Institute Programs The Emergency Management Institute (EMI) offers several programs that are designed for people who have emergency management responsibilities or meet the criteria specified at the web site cited below. The training is free of charge, however, individuals from private sector or contractors to State, local or Tribal governments must pay their own transportation and lodging fees. EMI has an integrated training approach and we encourage individuals from private sector to participate in our courses. EMI's programs include, but are not limited to the Master Trainer Program, Master Exercise Practitioner Program, Professional Development Series, Applied Practices Series and FEMA's Higher Education Program. For more information, see http://www.training.fema.gov/Programs/ or call (301) 447-1286.

FEMA Learning Resource Center (LRC) provides current information and resources on fire, emergency management and other all-hazards subjects. With its collection of more than 180,000 books, reports, periodicals, and audiovisual materials, the LRC houses the most extensive collection of fire service literature in the United States. Internet users may access the LRC's Online Public Access Catalog to perform literature searches and download over 17,000 documents. The LRC's collection of books and research reports may also be accessed by requesting interlibrary loan through a local library. For more information visit http://www.lrc.fema.gov or contact the program via phone (800) 638-1821 or by e-mail netclrc@dhs.gov.

U.S. Fire Administration's National Fire Academy Training Programs enhance the ability of fire and emergency services and allied professionals to deal more effectively with fire and related emergencies. NFA offers courses in the following subject areas: Arson Mitigation, Emergency Medical Services, Executive Development, Fire Prevention: Management, Fire Prevention: Public Education, Fire Prevention: Technical, Hazardous Materials, Incident Management, Management Science, Planning and Information Management and Training Programs. NFA offers residential training at its Emmitsburg, Maryland facility and off-campus training throughout the United States, as well as online self-study courses free of charge. For more information, see http://www.usfa.dhs.gov/nfa/index.shtm or call (301) 447-1000.

First Responder Training & Exercise Integration are delivered in the following formats: Resident – Instructor-led classroom training is provided at a training facility; Mobile – Also referred to as non-resident, mobile training can be performed by FEMA funded instructors at any location; Web-Based – Web-based or 'online' training is done via the internet and is often self-paced (no instructor); or Indirect – Indirect training includes training courses taught by instructors (non FEMA or training partner staff) that have completed 'Train the Trainer' courses. For more information, visit www.firstrespondertraining.gov or contact the program via phone (800) 368-6498 or e-mail askCSID@dhs.gov.

FEMA Alerts and Newsletters

FEMA Private Sector E-alert The FEMA Private Sector Division, Office of External Affairs, publishes periodic e-alerts providing timely information on topics of interest to private sector entities. The FEMA Private Sector Web Portal aggregates FEMA's online resources for the private sector. Content includes best 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 visit www.fema.gov/privatesector or sign up for the alert at FEMA-Private-Sector-Web@dhs.gov.

Citizen Corps E-mail Alerts provide weekly Community Preparedness news and events from various departments of the federal government and our national Citizen Corps partners and affiliates. For more information, visit www.citizencorps.gov or sign up for the alert at citizencorps@dhs.gov.

FEMA Publications

FEMA Library is a searchable web-based collection of all publicly accessible FEMA information resources, including thousands of CDs, DVDs, audio tapes, disability resources, posters, displays, brochures, guidance, policy papers, program regulations, guidelines, and forms. Users can search the collection by Subject, Audience Category including categories specific to private sector audiences, Hazard Type and other categories. For more information, visit http://www.fema.gov/library/ or call (800) 480-2520.

FEMA Programs and Services

Community Preparedness – Citizen Corps is FEMA's grassroots strategy to bring together government and community leaders to involve citizens in all-hazards emergency preparedness and resilience. Citizen Corps asks each individual to embrace the personal responsibility to be prepared; to get training in first aid and emergency skills; and to volunteer to support local emergency responders, disaster relief, and community safety. There are currently 2,433 Councils which serve over 227 million people or 80% of the total U.S. population. For more information on how you can participate, e-mail citizencorps@dhs.gov or visit www.citizencorps.gov.

Donations and Volunteers Information FEMA offers information on the best way to volunteer and donate during disaster response and recovery. For more information, see www.fema.gov/donations.

DisasterAssistance.gov DisasterAssistance.gov is a secure, user-friendly U.S. government web portal that consolidates disaster assistance information in one place. If you need assistance following a presidentially declared disaster that has been designated for individual assistance, you can now to go to www.DisasterAssistance.gov to register online. Local resource information to help keep citizens safe during an emergency is also available. Currently, 17 U.S. government agencies, which sponsor almost 60 forms of assistance, contribute to the portal. For web site technical assistance, contact (800) 745-0243.

The Emergency Lodging Assistance Program provides prompt lodging payments for short term stays in the event of a declared disaster. The program is administered by Corporate Lodging Consultants, a federal government contractor and the largest outsourced lodging services provider in North America. For more information, see http://ela.corplodging.com/programinfo.php, contact femahousing@corplodging.com, or call (866) 545-9865.

The Emergency Food and Shelter National Board Program was created in 1983 to supplement the work of local social service organizations within the United States, both private and governmental, to help people in need of emergency assistance. This collaborative effort between the private and public sectors has provided over $3.4 billion in Federal funds during its 27-year history. For more information, visit http://www.efsp.unitedway.org/.

The 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 Flood Map Assistance Center (FMAC) provides information to the public about National Flood Insurance Program rules, regulations, and procedures. The FMAC is often the first point of contact between FEMA and various flood map users. The FMAC's goal is to provide the appropriate information to callers to help them understand the technical issues involved in a particular situation. In addition to taking incoming telephone calls, Map Specialists respond to mapping-related e-mail inquiries, and also review and process Letter of Map Amendment (LOMA), Letter of Map Revision Based on Fill (LOMR-F), and Letter of Determination Review (LODR) requests. There are available resources for Engineers/Surveyors, Insurance Professionals and Lenders, Floodplain Managers. For more information, call (877) FEMA-MAP (877-336-2627) or e-mail FEMAMapSpecialist@riskmapcds.com.

FEMA Regulatory Materials FEMA publishes its regulations, containing FEMA's procedures and

requirements on the public, in Title 44 of the Code of Federal Regulations (CFR). These regulations are typically open for public comment before they go into effect. The public can access the regulations that are currently in effect electronically, by selecting Title 44 from the drop down menu at http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=%2Findex.tpl. The public can submit and view comments submitted by other individuals at www.regulations.gov. For more information on Federal agency rulemaking, visit www.reginfo.gov or to contact FEMA regulatory officials e-mail FEMA-RULES@dhs.gov.

FEMA Small Business Program Small business vendors are routed to the FEMA Small Business Analyst for notification, support and processing. Small Business inquires can be sent to FEMA-SB@dhs.gov.

U.S. Fire Administration (USFA) Fire Prevention and Safety Campaigns delivers fire prevention and safety education programs to reduce the loss of life from fire-related hazards, particularly among the very young and older adults. The campaigns encourage Americans to practice fire safety and to protect themselves and their families from the dangers of fire. In addition, they provide dedicated support to public fire educators and the media to facilitate community outreach to targeted audiences. For more information, visit http://www.usfa.dhs.gov/campaigns/ or call (301) 447-1000.

U.S. Fire Administration Publications encourage Americans including private sector constituents to practice fire safety and protect themselves and their families from the dangers of fire. Order online at http://www.usfa.dhs.gov/applications/publications/ or contact the U.S Fire Administration via e-mail, usfa-publications@dhs.gov or phone, (800) 561-3356.

Freight Rail Security Grant Program funds freight railroad carriers and owners and officers of railroad cars to protect critical surface transportation infrastructure from acts of terrorism, major disasters and other emergencies. For more information, visit http://www.fema.gov/government/grant/ or contact the program by e-mail, askcsid@dhs.gov or phone, (800) 368-6498.

Intercity Bus Security Grant Program provides funding to create a sustainable program for the protection of intercity bus systems and the traveling public from terrorism. The program seeks to assist operators of fixed-route intercity and charter bus services in obtaining the resources required to support security measures such as enhanced planning, facility security upgrades and vehicle and driver protection. For more information, visit http://www.fema.gov/government/grant/ or contact the program at askcsid@dhs.gov or (800) 368-6498.

Intercity Passenger Rail Grant Program creates a sustainable, risk-based effort to protect critical surface transportation infrastructure and the traveling public from acts of terrorism, major disasters and other emergencies within the Amtrak rail system. For more information visit http://www.fema.gov/government/grant/ or contact the program at askcsid@dhs.gov or (800) 368-6498.

National Dam Safety Program Led by FEMA, the National Dam Safety Program (NDSP) is a partnership of the States, Federal agencies, and other stakeholders to encourage individual and community responsibility for dam safety. Since the inception of the NDSP in 1979, FEMA has supported a strong, collaborative training program for dam safety professionals and dam owners. With NDSP training funds, FEMA has been able to expand existing training programs, begin new initiatives to keep pace with evolving technology, and enhance the sharing of expertise between the federal and state sectors. For more information, visit http://www.fema.gov/plan/prevent/damfailure/ndsp.shtm or http://www.damsafety.org/.

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. Web site: www.fema.gov/nims. Questions regarding NIMS should be directed to FEMA-NIMS@dhs.gov or (202) 646-3850.

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 incidents that range from the serious but purely local, to large-scale terrorist attacks or catastrophic natural disasters. For more information, visit http://www.fema.gov/nrf.

National Flood Insurance Program focuses on Flood Insurance, Floodplain Management and Flood Hazard Mapping. Nearly 20,000 communities across the U.S. and its territories participate in the NFIP by adopting and enforcing floodplain management ordinances to reduce future flood damage. In exchange, the NFIP makes Federally-backed flood insurance available to homeowners, renters, and business owners in these communities. See www.floodsmart.gov Flood insurance agents interested in the program please visit www.agents.floodsmart.gov or e-mail asktheexpert@riskmapcds.com.

Nonprofit Security Grant Program provides funding support for target-hardening activities to nonprofit organizations that are at high risk of a terrorist attack and are located within one of the specific UASI-eligible urban areas. It is also designed to promote coordination and collaboration in emergency preparedness activities among public and private community representatives, State and local government agencies, and Citizen Corps Councils. For more information, visit http://www.fema.gov/government/grant/nsgp or contact the program by e-mail, askcsid@dhs.gov or phone, (800) 368-6498.

Port Security Grant Program is a sustainable, risk-based effort to protect critical port infrastructure from terrorism, particularly attacks using explosives and non-conventional threats that could cause major disruption to commerce. The PSGP provides grant funding to port areas for the protection of critical port infrastructure from terrorism. This program is primarily intended to assist ports in enhancing maritime domain awareness; enhancing risk management capabilities to prevent, detect, respond to and recover from attacks involving improvised explosive devices, Chemical, Biological, Radiological, Nuclear,

Explosive, and other non-conventional weapons; providing training and exercises; and Transportation Worker Identification Credential implementation. For more information, visit http://www.fema.gov/government/grant/ or contact the program by e-mail, askcsid@dhs.gov or phone, (800) 368-6498.

QuakeSmart is designed to encourage business leaders and owners in areas of the U.S. that are at risk from earthquakes to take actions that will mitigate damage to their businesses, provide greater safety for customers and employees, and speed recovery in the event of an earthquake. The goal of QuakeSmart is to build awareness within the business community of the risk and to educate businesses, particularly small and emerging businesses, on the relatively simple things they can do to reduce or mitigate the impact of earthquakes, and support community preparedness. Business leaders and owners interested in finding out how to reduce or mitigate the impact of earthquakes on their business should visit www.quakesmart.org.

Ready Business The U.S. Department of Homeland Security and the Advertising Council launched the *Ready Business* Campaign in September 2004. This extension of the successful *Ready* Campaign, *Ready Business* helps owners and managers of small- and medium-sized businesses prepare their employees, operations and assets in the event of an emergency. For free tools and resources, including how to create a business emergency plan, please visit www.ready.gov.

Radiological Emergency Preparedness Program (REP) Program helps to secure the health and safety of citizens living around commercial nuclear power plants. REP is responsible for reviewing and approving all community radiological emergency plans. The REP program is a leader in areas of policy guidance, planning, training, public education and preparedness for nuclear power plants. For over three decades, local and state responders have relied on REP's leadership to correct preparedness plans, monitor rigorous training regimens and support effective performance in the unlikely event of a radiological emergency. For more information, visit http://www.fema.gov/hazard/nuclear/index.shtm.

Technical Assistance (TA) Program seeks to build and sustain capabilities through specific services and analytical capacities through the development, delivery, and management of TA services that support the four homeland security mission areas (i.e. prevention, protection, response, and recovery), in addition to homeland security program management. TA is offered to a wide variety of organizations and grantees through an extensive menu of services responsive to national priorities. To best accommodate the wide variety of TA needs and deliverables, three levels of TA are provided. Level I/II services can be made available to private sector organizations and includes general information, models, templates, and samples. Level III services, available to private sector organizations who may be DHS grantees, provides onsite support via workshops and interaction between TA providers and recipients. For more information, visit http://www.fema.gov/about/divisions/pppa_ta.shtm or contact (800) 368-6498 or e-mail FEMA-TARequest@fema.gov.

Transit Security Grant Program is a sustainable, risk-based effort to protect critical surface transportation infrastructure and the traveling public from acts of terrorism, major disasters, and other emergencies. For more information, visit http://www.fema.gov/government/grant/ or contact the program by e-mail, askcsid@dhs.gov or phone, (800) 368-6498.

Tornado Safety Initiative assesses building damages and identifies lessons learned after tornadoes occur; funds research on shelter design and construction standards; develops best practices and technical manuals on safe rooms and community shelters; and produces public education materials on tornado preparedness and response. FEMA produces technical manuals for engineers, architects, building officials, and prospective shelter owners on the design and construction of safe rooms and community shelters. For more information, visit http://www.fema.gov/plan/prevent/saferoom/index.

Unified Hazard Mitigation Assistance (HMA) Grant Programs present a critical opportunity to reduce the risk to individuals and property from natural hazards while simultaneously reducing reliance on Federal disaster funds. While the statutory origins of the programs differ, all share the common goal of reducing the risk of loss of life and property due to natural hazards. HMA programs are subject to the availability of appropriation funding or funding based on disaster recovery expenditures, as well as any directive or restriction made with respect to such funds. HMA programs include Hazard Mitigation Grant Program, Pre-Disaster Mitigation program, Flood Mitigation Assistance program, Repetitive Flood Claims (RFC) program and Severe Repetitive Loss program. See www.fema.gov/government/grant/hma/index.shtm.

U.S. Immigration and Customs Enforcement (ICE)

U.S. Immigration and Customs Enforcement (ICE) is the largest investigative agency in the U.S. Department of Homeland Security (DHS). Formed in 2003 as part of the federal government's response to the 9/11 attacks, ICE's mission is to protect the security of the American people and the homeland by vigilantly enforcing the nation's immigration and customs laws. ICE combines innovative investigative techniques, new technological resources and a high level of professionalism to provide a wide range of resources to the public and to our Federal, State and local law enforcement partners. www.ice.gov

Forced Labor Resources The ICE Office of International Affairs investigates allegations of forced labor in violation of the Tariff Act of 1930 (Title 19 USC §1307). To request more information or a copy of A Forced Child Labor Advisory booklet and brochure, please contact: ice.forcedlabor@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 to the United States; a detailed description of the product; all pertinent facts known regarding the production of the merchandise abroad. For the location of ICE foreign offices, go to the ICE web site at http://www.ice.gov, click *About Us*, click *Office of International Affairs* and select your country. ICE maintains a 24/7 hotline at (866) DHS-2-ICE.

Human Rights Violators and War Crimes Center has a mission to protect the public by targeting war criminals and those who violate human rights, including violators living both domestically and abroad. The assigned staff of ICE investigators and intelligence analysts dedicated to the Center work with governmental and non-governmental agencies. They 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.

Human Trafficking: "Hidden in Plain Sight" is the ICE human trafficking public outreach campaign that heightens awareness of human trafficking through announcements via billboards and posters on public transportation, bus stops and in businesses. The Hidden in Plain Sight campaign provides critical human trafficking information to the public and gives people a method for reporting suspected human trafficking activity. ICE's Office of Investigations (OI) designed a one-minute video Public Service Announcement (PSA), which is a broadcast message used for public outreach. ICE uses the PSA during presentations to provide information to the general public and human trafficking-related organizations. The PSA is accessible to the public via the ICE Web site at www.ice.gov and it is also distributed to the public on DVD during training and presentations worldwide. See the flash video at http://www.ice.gov/flashmovie/human-trafficking/plain-sight.htm.

Human Trafficking: Indicators Pamphlet is currently produced in English, Spanish, and Portuguese and is distributed during presentations and trainings worldwide. See http://www.ice.gov/pi/news/factsheets/humantrafficking.htm.

Human Trafficking: Awareness Resources ICE is the primary agency within the Department of Homeland Security that fights human trafficking. Trafficking in Persons (TIP) is a modern day form of slavery. Human trafficking is defined by Section 103 of the Trafficking Victims Protection Act of 2000 as '(A) sex trafficking in which a commercial sex act is induced by force, fraud, or coercion, or in which the person induced to perform such act has not attained 18 years of age; or (B) the recruitment, harboring, transportation, provision, or obtaining of a person for labor or services, through the use of force, fraud, or coercion for the purpose of subjection to involuntary servitude, peonage, debt bondage, or slavery. ICE is committed to a victim-focused approach to trafficking investigations that places equal importance on protecting the victims and prosecuting the traffickers. Part of this strategy includes an aggressive public outreach campaign to raise awareness of the issue and provide a mechanism for the public to report suspected trafficking activity. ICE also conducts continuous outreach and training to U.S. and foreign law enforcement, non-governmental and international organizations, in order to provide awareness and the latest investigative techniques and victim assistance practices. The public is encouraged to report all suspicious activity to ICE at (866) DHS-2ICE (1-866-347-2423). Informational material on human trafficking is produced in a variety of languages, and is available to law enforcement, NGOs and includes the following: a public service announcement; human trafficking brochure; human trafficking indicator wallet cards; and human trafficking indicators for law enforcement brochure. See http://www.ice.gov/pi/investigations/publicsafety/humantrafficking.htm.

Human Trafficking: Trafficking in Persons (TIP) Card ICE currently distributes human trafficking material, known as the human trafficking in persons **(**TIP) card. This plastic business card helps distinguish between the crime of human trafficking versus the crime of human smuggling, listing indicators of each as the two crimes are often confused. The TIP card includes the ICE telephone number for individuals to call for guidance or to report suspicious activity. The TIP card is currently produced in 17 different languages. To request the TIP card, contact your local ICE office. The TIP cards are also distributed during presentations and training offered worldwide. For more information visit the ICE Web site at www.ice.gov. For ICE principal field offices across the country, see http://www.ice.gov/about/investigations/contact.htm.

ICE LINK Portal The ICE National Incident Response Unit (NIRU) for incident awareness, continuity of operations, exercises, incident response, special event coordination and many other homeland security requirements administers a web-based communications and collaboration platform called the ICE LINK Portal. The ICE LINK Portal is a robust, sensitive but unclassified, information-sharing network used as a force multiplier to enhance coordination with Federal, State, local and Tribal

priorities. ICE LINK Portal users include federal agencies, fusion centers, military components, Interpol and the intelligence community. Additionally, the ICE LINK Portal can be used for Critical Infrastructure and Key Resources (CI/KR) first responder personnel in the private sector in the event of a national crisis or incident. For more information and/or assistance, contact NIRU at niru@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. More information can be found at ICE's Web site at www.ice.gov/image. Contact: IMAGE@dhs.gov or Section Chief Adam Wilson at (202) 732-3064.

ICE Office of Public Affairs (ICE OPA) is dedicated to building understanding and support for the agency's mission through outreach to DHS employees, the media and the general public. ICE OPA is headquartered at Potomac Center North (PCN), 500 12th St. SW, in Washington, D.C. ICE field public affairs officers are located thoughout 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, (202) 732-4242.

ICE Privacy Office sustains privacy protections and the transparency of government operations while supporting the ICE mission. The ICE Privacy Office ensures that the Privacy Impact Assessments and System of Records Notices complies with key federal privacy laws and policies. Members of the public can contact the Privacy Office with concerns or complaints regarding their privacy in regard to the mission of ICE. See http://www.ice.gov/about/privacyoffice/contact.htm. For more information, contact ICEPrivacy@dhs.gov, (202) 732-3300.

ICE Tip-Line is a 24/7 toll free number enabling the public to report violations of customs and immigration laws, sexual and economic exploitation of children and adults, threats to national security and other activities considered illegal or suspicious in nature. Please assist DHS in maintaining the security and integrity of the nation by reporting illegal activity. More information regarding ICE programs can be found at the ICE Web site http://www.ice.gov or http://www.ice.gov/pi/topics/index.htm or by calling **(866) DHS-2ICE** (1-866-347-2423) or outside the United States: +1 (877) 347-2423.

ICE Victim Assistance Program (VAP) provides information and assistance to human trafficking victims. The VAP provides information about post-correctional release or removal of criminal aliens from ICE custody. The VAP provides brochures for victims of trafficking and its victim notification program. To request copies of the brochures, please contact the VAP at (866) 872-4973.

The National Intellectual Property Rights (IPR) Coordination Center is the federal government's central point of contact in the fight against IPR violators and the flow of counterfeit goods into the United States since 2000. The new center in Northern Virginia is the high-tech home of a partnership between government, private industry and law enforcement communities. More information can be found at http://www.ice.gov/pi/iprctr/index.htm. Report an IPR violation at http://www.ice.gov/partners/cornerstone/ipr/IPRForm.htm or contact the IPR Center at (866) IPR-2060 or (866) 477-2060.

Money Laundering and Operation Cornerstone U.S. Immigration and Customs Enforcement (ICE) recognizes that the private sector represents America's first line of defense against money laundering. In Operation Cornerstone, the ICE Office of Investigations reaches out to the U.S. business community, along with State and Federal agencies to combat financial and trade crimes. Operation Cornerstone 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 ICE Financial Programs/Cornerstone Unit 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 visit: www.ice.gov/cornerstone. Report suspicious activity by calling (866) DHS-2-ICE.

Project Shield America (PSA) is the first line of defense against those who compromise U.S. national security by violating export laws, sanctions and embargoes. Specifically, ICE's Counter-Proliferation Investigations Unit reaches out to applicable high-tech industries to monitor weapons of mass destruction and their components that are potential targets for illegal trafficking. Through PSA, ICE works in partnership with U.S. Customs and Border Protection (CBP) and U.S. companies that manufacture, sell or export strategic technology and munitions. See http://www.ice.gov/doclib/investigations/pdf/cpi_brochure.pdf (pdf 192 KB). For additional information, please contact ICE Headquarters, PSA Program Manager at ICE Headquarters at (202) 732-3765 or (202) 732-3764. Report suspicious activity at the ICE tip line (866) DHS-2-ICE (1-866-347-2423).

Student and Exchange Visitor Program (SEVP) was established in 2003 as the Department of Homeland Security's front line effort to ensure that the student visa system is not exploited by those wishing to do harm to the United States. SEVP's key tool in this effort is the Student and Exchange Visitor Information System (SEVIS), a web-based information management system that allows ICE to monitor the status of non-immigrant student and exchange visitors in the United States. SEVP collects, maintains and provides the information 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, U.S. Customs and Border Protection, U.S. Citizenship and Immigration Services, and ICE. For more information, visit http://www.ice.gov/sevis/. For inquiries by phone, call the SEVP Response Center at (703) 603-3400 or via e-mail at: SEVIS.Source@DHS.gov.

Office of Infrastructure Protection (IP)

From energy systems that power our neighborhoods, to transportation networks that move us around our communities and the country, to facilities that provide our families with safe drinking water, critical infrastructure and key resources (CIKR) impact nearly every aspect of our daily lives. In short, CIKR is an umbrella term referring to the assets of the United States essential to the nation's security, public health and safety, economic vitality, and way of life. CIKR is divided into 18 separate sectors, as diverse as agriculture and food, emergency services, and cyber networks. Because this critical infrastructure provides our country with the enormous benefits and services and opportunities on which we rely, we are very mindful of the risks posed to CIKR by terrorists, pandemic diseases and natural disasters. At the Department of Homeland Security, we know that these threats can have serious effects, such as cutting populations off from clean water, power, transportation, or emergency supplies. Secretary Napolitano is working to raise awareness about the importance of our nation's critical infrastructure and to strengthen our ability to protect it. The Department oversees programs and resources that foster public-private partnerships, enhance protective programs, and build national resiliency to withstand natural disasters and terrorist threats. www.dhs.gov/criticalinfrastructure

IP Training and Education

Active Threat Recognition for Retail Security Officers This 85-minute presentation produced by the Office for Bombing Prevention is split into easy to understand modules and uses specific foreign and domestic case studies to explain lessons learned and to discuss specific considerations for retail and shopping centers. The training discusses signs of criminal and terrorist activity; types of surveillance; and suspicious behavioral indicators. The presentation is available with guest log-in capabilities on the DHS Homeland Security Information Network (HSIN). To access the presentation, please register at: https://connect.hsin.gov/attrrso/event/registration.html After submitting the short registration information to include setting a password of your choice, you will receive an e-mail confirmation with instructions for logging in to view the material. For more information, contact the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

Bomb Event Management Web Training is a 60-minute online session produced by the Office for Bombing Prevention that provides an overview of risks and risk mitigation considerations related to improvised explosive devices (IED) threats and planning. This web training 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, contact the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

Bombing Prevention Workshop is a one-day workshop, intended for regional level public and private stakeholders and planners from emergency management, security, and law enforcement, designed to enhance the effectiveness in managing a bombing incident. This workshop reviews the current development of strategies and brings together best practices from regions across multiple localities, disciplines and levels of government. The guided scenario discussion establishes the foundation for the stakeholders within the region to implement a Bombing Prevention Plan. This workshop can accommodate up to 50 participants. To request training contact the DHS Office for Bombing Prevention at OBP@dhs.gov, (703) 235-5723.

Chemical Sector Explosive Threat Awareness Training Program The Chemical Sector-Specific Agency (SSA) is offering a series of one day vehicle borne improvised explosive device (VBIED) training sessions to chemical facility security officers. This course is offered in six locations in FY10 (Dallas, Orlando, New Orleans, St. Louis, Seattle, and Buffalo). Contact the Chemical SSA for more information ChemicalSector@dhs.gov.

Counterterrorism Protective Measures Course is a two-day course designed to enhance Commercial Sector awareness on how to devalue, detect, deter, and defend facilities from terrorism, by providing the knowledge and skills necessary in understanding common vulnerabilities and employing effective protective measures. The Protective Measures Course includes lessons learned and industry best practices in mitigating terrorist attacks. It serves as a follow-up to the Soft Target Awareness Course, focusing more on implementation than awareness. This course can accommodate 35 participants. To request training, contact the DHS Office for Bombing Prevention, OBP@dhs.gov, (703) 235-5723.

Critical Infrastructure and Key Resources (CIKR) Learning Series features one-hour infrastructure protection (IP) Web-based seminars on current topics and issues of interest to CIKR owners and operators and key government partners. Over 5,000 partners/stakeholders have registered for the Learning Series since its inception in August, 2008. The list serve for this series includes more than 27,000 interested individuals. See http://www.dhs.gov/files/programs/gc_1231165582452.shtm. For more information, contact IP_Education@hq.dhs.gov.

Critical Infrastructure and Key Resources (CIKR) Training Module provides an overview of the National Infrastructure Protection Plan (NIPP) and CIKR Annex to the National Response Framework. The module was developed for inclusion in the FEMA Integrated Emergency Management and other incident management related courses. This document is available upon request in PowerPoint format with instructor and participant guides and can be easily integrated into existing training programs. A Spanish version is also available. To request the training module, contact IP_Education@hq.dhs.gov.

DHS/Commercial Facilities Training Resources Guide pamphlet was developed to promote classroom and independent study programs for DHS partners and private sector stakeholders that build functional skills for disaster response effectiveness. Subject matter includes cybersecurity, weapons of mass destruction, and natural disaster planning. Available on request, contact the

Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

DHS Retail Video: "What's in Store - Ordinary People/Extraordinary Events" is a multimedia training video for retail employees of commercial shopping venues alerting them to the signs of suspicious behavior in the workplace that might lead to a catastrophic act. See http://www.dhs.gov/multimedia/dhs_retail_video.wmv. For more information, contact the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

DHS Training Video "Check It!: Protecting Public Spaces" is a training video for front line event staff at large public venues. The video demonstrates the proper procedures for conducting bag searches and recognizing suspicious behavior at public gathering spaces like sports venues. The video is available for viewing and download at http://www.dhs.gov/files/programs/gc_1259859901230.shtm#4 or by contacting the Commercial Facilities Sector-Specific Agency at CFSTeam@hq.dhs.gov.

Emergency Services Sector Training Catalog describes public and private resources and programs that are applicable to first responders. Printed catalogs are available by contacting the Emergency Services Sector-Specific Agency ESSTeam@hq.dhs.gov.

Improvised Explosive Device (IED) Awareness / Bomb Threat Management Workshop IED attacks remain the primary tactic for bombers, terrorists, and criminals seeking relatively uncomplicated, inexpensive means for inflicting mass casualties and maximum damage. This four-hour presentation is designed to enhance and strengthen the participant's knowledge, skills, and abilities in relation to the threat of IEDs. The information presented outlines specific practices associated with Bomb Threat Management including IED awareness, explosive incidents, and bombing prevention. This workshop is designed to provide two four-hour sessions, morning and afternoon, with 50 participants for each session. To request training, contact the DHS Office for Bombing Prevention at OBP@dhs.gov, (703) 235-5723.

Improvised Explosive Device (IED) Awareness Web Training This 60-minute IED Awareness Web Training, produced by the Office for Bombing Prevention and similar to the IED Awareness Course, is designed to enhance and strengthen the participant's knowledge, skills, and abilities in relation to the threat of IEDs. Topics addressed during the web training include the use of IEDs as a popular terrorist attack method; types of explosives and explosive effects; construction, components, and categories of IEDs; and IED related safety measures. This web training 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, contact the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

Improvised Explosive Device (IED) Search Procedures Workshop This 8-hour Workshop, consisting of lecture and practical exercises, is designed for security personnel and facility managers of sites hosting any event that requires increased IED security preparedness. The information provided during the Workshop focuses on general safeties used for specialized explosives searches and sweeps, and can be tailored to meet the requirements for supporting any event. The Workshop can accommodate 25 participants. To request training, contact the DHS Office for Bombing Prevention: OBP@dhs.gov, (703) 235-5723.

Independent Study Course IS-821 "Critical Infrastructure and Key Resources (CIKR) Support Annex" provides an introduction to the CIKR 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.

Independent Study Course IS-860.a National Infrastructure Protection Plan (NIPP) presents an overview of the NIPP. The NIPP provides the unifying structure for the integration of existing and future CIKR 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.

Independent Study Course IS-870: Dams Sector: Crisis Management Overview is web-based training focused on information provided within the Dams Sector Crisis Management handbook. See http://training.fema.gov/EMIWeb/IS/IS870.asp. For more information, contact the Dams Sector-Specific Agency, dams@dhs.gov.

Integrated Common Analytical Viewer (iCAV) Web-based Training provides instruction on the use of the iCAV Next Generation geospatial visualization tool, including access and use of DHS geospatial resources and data. Users are guided through system "buttonology" to gain a feel for the types of imagery, infrastructure, and situational awareness data available through iCAV Next Generation, as well as some of the analytical tools that users can leverage to understand infrastructure in a domestic response context. More information on iCAV Next Generation is available at http://www.dhs.gov/icav, and the training itself is available at http://www.jsrts.org/dhs/icav.

Private Sector Counterterrorism Awareness Workshop is a one-day workshop designed to improve the knowledge of private sector security professionals by providing exposure to key elements of soft target awareness, surveillance detection, and improvised explosive device (IED) recognition. The workshop's training materials enhance and reinforce participants' knowledge, skills, and abilities related to preventing, protecting against, responding to, and recovering from terrorist threats and incidents. The workshop outlines specific counterterrorism awareness and prevention actions that reduce vulnerability and mitigate the risk of domestic terrorist attacks. This workshop can accommodate 100 to 250 participants. To request training contact the DHS Office for Bombing Prevention, OBP@dhs.gov at (703) 235-5723.

Soft Target Awareness Course is designed to enhance individual and organizational awareness of terrorism and help facilitate information sharing at commercial facilities considered soft targets, such as shopping malls and hotels. Commercial infrastructure facility managers, supervisors, operators, and security staff gain a better understanding of their roles in deterring, detecting, and defending their facilities from terrorism. Participants choose from five

focus areas according to their specific affiliation: Stadiums and Arenas; Places of Worship; Education; Malls and Shopping Centers; and Large Buildings, Hotels and Medical Facilities. Each of these focus areas is comprised of a four-hour session of combined informal lecture and capstone guided discussions. Each session can accommodate 35 participants or can be modified for one general session for up to 175 participants. To request training contact the DHS Office for Bombing Prevention at OBP@dhs.gov, (703) 235-5723.

Surveillance Detection Training for Commercial Infrastructure Operators and Security Staff Course is a three-day course that explains how protective measures can be applied to detect and deter potential threats to critical infrastructure and key resources (CIKR), as well as the fundamentals for detecting surveillance activity. The course is designed for commercial infrastructure operators and security staff of nationally significant CIKR facilities. This course can accommodate 25 participants. To request training contact the DHS Office for Bombing Prevention at OBP@dhs.gov, (703) 235-5723.

Surveillance Detection Training for Municipal Officials, State and Local Law Enforcement Course is a three-day course that provides the knowledge and skills necessary to establish surveillance detection operations to protect critical infrastructure and key resources (CIKR), during periods of elevated threat. Comprised of five modules of informal lecture and two exercises, it provides participants with an awareness of terrorist tactics and attack history and illustrates the means and methods to detect surveillance through practical surveillance detection exercises. This Surveillance Detection Course is designed for municipal security officials and State and local law enforcement with jurisdictional authority over nationally significant CIKR facilities. This course can accommodate 25 participants. To request training contact the DHS Office for Bombing Prevention, OBP@dhs.gov, (703) 235-5723.

Surveillance Detection Web Training is a 60-minute online session produced by the Office for Bombing Prevention that addresses the threat of hostile surveillance on critical infrastructure. Topics addressed during the web training include basic private sector threat awareness, surveillance and surveillance detection defined, recognition of the types and patterns of behavior associated with terrorist activity, signs of terrorist activity, and suspicious activity reporting. This web training 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, contact the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

Threat Detection and Reaction by Retail Staff (Point of Sale) This 20-minute presentation is intended for Point-of-Sale staff, but is applicable to all employees of a shopping center, mall, or retail facility. It uses case studies and best practices to explain suspicious behavior and items; how to reduce the vulnerability to an active shooter threat; and the appropriate actions to take if employees notice suspicious activity. To access the 20-minute presentation, visit: https://connect.hsin.gov/p21849699/.

Web-Based Chemical Security Awareness Training Program is an interactive tool available free to chemical facilities nationwide to increase security awareness. The training is designed for all facility employees, not just those traditionally involved in security. Upon completion, a certificate is awarded to the student. See https://www.chemicalsecuritytraining.com/. Contact the Chemical Sector-Specific Agency at 1-877-CHEMSEC, ChemicalSector@dhs.gov.

IP Guidance Documents/Publications

Active Shooter - How To Respond is a desk reference guide, a reference 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. See http://www.dhs.gov/files/programs/gc_1259859901230.shtm. For more information, contact the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

Bomb-making Materials Awareness Program (BMAP)/Suspicious Behavior Cards These joint FBI-DHS private sector advisory cards offer simple concise tips and images helping retailers identify and report suspicious activity and sale of household items that can be used in making home-made explosives (HMEs) and improvised explosive devices (IED). The register cards give front end store employees guidance on precursor materials and what to look for regarding suspicious purchases. See http://www.dhs.gov/files/programs/gc_1259938444548.shtm. To request materials or additional information, contact the DHS Office for Bombing Prevention at OBP@dhs.gov, (703) 235-5723.

Chemical Facility Anti-Terrorism Standards (CFATS) Frequently Asked Questions were developed and continue to be regularly updated as a means of assisting facilities in complying with the CFATS regulation. The FAQs are searchable and categorized to further benefit the user and can be found at http://csat-help.dhs.gov/pls/apex/f?p=100:1:7096251139780888. For more information, contact the CFATS Help Desk at cfats@dhs.gov, (866) 323-2957.

Chemical Facility Anti-Terrorism Standards (CFATS) Presentations The Infrastructure Security Compliance Division (ISCD) reaches out to people and companies in the chemical industry and those interested in chemical security. Those interested in a live presentation about CFATS by ISCD personnel can find more information about such presentations at DHS' chemical security web site: http://www.dhs.gov/files/programs/gc_1224766914427.shtm. For more information, contact the CFATS Help Desk at cfats@dhs.gov, (866) 323-2957.

Chemical Facility Anti-Terrorism Standards (CFATS) Risk-Based Performance Standards (RBPS) The Infrastructure Security Compliance Division (ISCD) provides outreach to key stakeholders with interest or involvement in chemical facility security. Those interested in a live presentation about CFATS by ISCD personnel can find more information and request a presentation by visiting http://www.dhs.gov/files/programs/gc_1224766914427.shtm. For more information, contact the CFATS Help Desk at cfats@dhs.gov, (866) 323-2957.

Chemical-Terrorism Vulnerability Information (CVI) is the information protection regime authorized by Section 550 of Public Law 109-295 to protect from inappropriate public

disclosure of any information developed or submitted pursuant to Section 550. This includes information that is developed and/or submitted to DHS pursuant to the Chemical Facility Anti-Terrorism Standards (CFATS) regulation which implements Section 550. See www.dhs.gov/chemicalsecurity. For more information, contact the CFATS Help Desk at csat@dhs.gov, (866) 323-2957.

Commercial Facilities Sector Pandemic Planning Documents for use by public assembly sector stakeholders detailing key steps and activities to take when operating during a pandemic influenza situation, a process tracking and status template, and a checklist of recommendations for pandemic response plan development. The products were created in partnership with International Association of Assembly Manager's Academy for Venue Safety and Security. Materials are available on request by contacting the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

Dams Sector Resources provide owners/operators with information regarding the Dams Sector. Publications include: **Dams Sector Consequence-Based Top Screen Fact Sheet, Dams Sector Councils Fact Sheet**, **Dams Sector Crisis Management Handbook** , **Dams Sector Exercises Series Fact Sheet - 2009**, **Dams Sector Overview Brochure, Dams Sector Security Awareness Guide, Security Awareness Guide for Levees**, **Security Awareness for Levee Owners Brochure, Dams Sector Standard Operating Procedures for Information Sharing**, **Waterside Barriers Guide, Suspicious Activity Reporting Fact Sheet, Personnel Screening Guide for Owners and Operators**, and **Physical Security Measures for Levees Brochure**. These resources are available on the HSIN-CS Dams Portal, https://cs.hsin.gov/C2/DS/default.aspx, the CIKR Resource Center, http://www.dhs.gov/criticalinfrastructure, and the Association of State Dam Safety Officials (ASDSO) Web site, http://www.damsafety.org. For more information, contact the Dams Sector-Specific Agency at dams@dhs.gov.

Dams Sector Resources (For Official Use Only): The **Dams Sector Security Awareness Handbook** assists owners/operators in identifying security concerns, coordinating proper response, and establishing effective partnerships with local law enforcement and first responder communities. The **Dams Sector Protective Measures Handbook a**ssists owners/operators in selecting protective measures addressing the physical, cyber, and human elements and includes recommendations for developing site security plans. The **Dams Sector Research & Development Roadmap: Development of Validated Damage and Vulnerability Assessment Capabilities for Aircraft Impact Scenarios** is a collaborative effort involving multiple agencies focused on investigating vulnerabilities of concrete arch and embankment dams to aircraft impact scenarios. These For Official Use Only (FOUO) documents are available to vetted private sector critical infrastructure owners and operators with a demonstrated need to know. For more information, contact the Dams Sector-Specific Agency at dams@dhs.gov.

DHS Daily Open Source Infrastructure Report is collected each week day as a summary of open-source published information concerning significant critical infrastructure issues. Each Daily Report is divided by the critical infrastructure sectors and key assets defined in the National Infrastructure Protection Plan. The DHS Daily Open Source Infrastructure Report is available on DHS.gov and Homeland Security Information Network-Critical Sectors (HSIN-CS). See http://www.dhs.gov/files/programs/editorial_0542.shtm. For more information, contact NICCReports@dhs.gov or CIKR.ISE@dhs.gov or (202) 312-3421.

DHS Retail Video: "What's in Store - Ordinary People/Extraordinary Events" is a multimedia training video for retail employees of commercial shopping venues alerting them to the signs of suspicious behavior in the workplace that might lead to a catastrophic act. See http://www.dhs.gov/multimedia/dhs_retail_video.wmv. For more information, contact the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

Education, Outreach, and Awareness Snapshot The National Infrastructure Protection Plan (NIPP) provides the coordinated approach for establishing national priorities, goals, and requirements for critical infrastructure and key resources (CIKR) protection and resilience. The NIPP also establishes a framework that allows people and organizations to develop and maintain key CIKR protection expertise. This two-page snapshot describes the NIPP's approach to building national awareness and enabling education, training, and exercise programs. See http://www.dhs.gov/xlibrary/assets/nipp_education.pdf. For additional information, contact NIPP@dhs.gov.

Emergency Services Personal Readiness Guide for Responders and Their Families is a tri-fold handout providing a description of the Ready Campaign, the Emergency Services Sector-Specific Agency, a list of website resources and instructions on family preparedness that include suggestions on developing an emergency kit and family emergency plan. The **Emergency Services Sector (ESS) Video** is a three-minute video providing an overview of the ESS Sector. The video is appropriate for conferences and events to grow awareness and participation in sector activities. For more information, or to request materials contact the Emergency Services Sector-Specific Agency at ESSTeam@hq.dhs.gov.

Evacuation Planning Guide for Stadiums was developed to assist stadium owners and operators with preparing an Evacuation Plan and determining when and how to evacuate, conduct shelter-in-place operations, or relocate stadium spectators and participants. The NASCAR Mass Evacuation Planning Guide and Template was modified into an Evacuation Planning Guide for Stadiums by a working group composed of various Federal agencies and members of the Commercial Facilities Sector Coordinating Council. See http://www.dhs.gov/xlibrary/assets/ip_cikr_stadium_evac_guide.pdf. For more information, contact the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

Guide to Critical Infrastructure and Key Resources (CIKR) Protection at the State, Regional, Local, Tribal, & Territorial Level outlines the attributes, capabilities, needs, and processes that a State or local government entity should include in establishing its own CIKR protection function such that it integrates with the National Infrastructure Protection Plan (NIPP) and accomplishes the desired local benefits. This document is available by contacting the NIPP Program Management Office at NIPP@dhs.gov.

Hotel and Lodging Advisory Poster was created for all staff throughout the U.S. Lodging Industry designed to increase awareness regarding a property's potential to be used for illicit purposes; suspicious behavior and items; and appropriate actions for employees to take if they notice suspicious activity. The poster was designed in tandem with the Commercial Facilities Sector Coordinating Council and the Lodging Subsector. See http://www.dhs.gov/xlibrary/assets/ip_cikr_hotel_advisory.pdf. For additional information, contact the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

Infrastructure Data Taxonomy (IDT) Critical infrastructure and key resources (CIKR) and their elements can be described and categorized in various ways, which can result in inconsistent communication and hinder timely decision-making within the homeland security community. To prevent such problems, the Department of Homeland Security uses an Infrastructure Data Taxonomy to enable transparent and consistent communication about CIKR between government and private sector partners with its structured terminology, the Infrastructure Data Taxonomy allows its users to designate an asset as belonging to a particular group, and then apply additional, associated taxonomy levels to detail the specifics of the asset and describe its functions. By applying a detailed, structured system of categorization to assets that includes sectors, sub-sectors, segments, sub-segments and asset type, the Infrastructure Data Taxonomy minimizes potential confusion and enhances transparency about CIKR. See http://www.dhs.gov/files/publications/gc_1226595934574.shtm. To request access to download, view, and comment on the Infrastructure Data Taxonomy please visit https://lens.iac.anl.gov/dana-na/auth/url_31/welcome.cgi. Contact: IICD@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, private sector CIKR owners and operators should contact DHS Office of Infrastructure Protection Vulnerability Assessments Branch at IPassessments@dhs.gov or the DHS Protective Security Advisor (PSA) Field Operations Staff: PSAFieldOperationsStaff@hq.dhs.gov or (703) 235-5724.

International Issues for Critical Infrastructure and Key Resources (CIKR) Protection 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. This two-page snapshot describes the approach to international issues embodied in the NIPP and the Sector-Specific Plans. See http://www.dhs.gov/xlibrary/assets/nipp_consolidated_snapshot.pdf. For more information, contact NIPP@dhs.gov.

Multi-Jurisdiction Improvised Explosive Device (IED) Security Plan (MJIEDSP) An effective response to bombing threats and actual incidents requires the close coordination of many different public safety and law enforcement organizations and disciplines. MJIEDSP assists multi-jurisdiction areas in developing a detailed IED security plan that integrates the assets and capabilities of multiple jurisdictions and emergency service sectors. To request additional information, contact the DHS Office for Bombing Prevention at OBP@dhs.gov, (703) 235-5723.

National Critical Infrastructure and Key Resources (CIKR) Protection Annual Report Snapshot Homeland Security Presidential Directive 7, which directed the development of the National Infrastructure Protection Plan, also designated 17 Federal Sector-Specific Agencies (SSAs) and required each SSA to provide an annual report to the Secretary of Homeland Security on their efforts to identify, prioritize, and coordinate CIKR protection in their respective sectors. This two-page snapshot describes the National CIKR Protection Annual Report that is developed from the Sector Annual Reports. See http://www.dhs.gov/xlibrary/assets/nipp_annrpt.pdf. For more information, contact NIPP@dhs.gov.

National Infrastructure Protection Plan (NIPP) 2009 provides the unifying structure for the integration of a wide range of efforts for the enhanced protection and resiliency of the nation's critical infrastructure and key resources (CIKR) into a single national program. See http://www.dhs.gov/files/programs/editorial_0827.shtm The **NIPP 2009 Overview Snapshot** provides a brief overview of the NIPP risk management framework and the sector partnership model. See http://www.dhs.gov/xlibrary/assets/nipp_consolidated_snapshot.pdf. The **NIPP Brochure** describes the national approach to achieving the goals articulated in the NIPP, the NIPP risk management framework, the NIPP value proposition, and the sector partnership model. The **NIPP Information Sharing Snapshot** describes the NIPP's approach to achieving active participation by government and private sector partners through robust multi-directional information sharing. It describes the networked approach to information sharing under the NIPP and the establishment of the CIKR Information-Sharing Environment (CIKR ISE). See http://www.dhs.gov/xlibrary/assets/NIPP_InfoSharing.pdf. For more information or to request materials contact the NIPP Program Management Office NIPP@dhs.gov.

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.

Planning for 2009 H1N1 Influenza: A Preparedness Guide for Small Business The Department of Homeland Security, the Center for Disease Control (CDC), and the Small Business Administration have developed this booklet to help small businesses understand what impact a new influenza virus, like 2009 H1N1 flu, might have on their operations, and how important it is to have a written plan for guiding your business through a possible pandemic. See http://www.flu.gov/professional/business/

smallbiz.html. For more information, contact IP_Education@hq.dhs.gov.

Protective Measures Guide for U.S. Sports Leagues provides an overview of best practices and protective measures designed to assist sports teams and owners/operators of sporting event venues with planning and managing security at their facility. The Guide provides examples of successful planning, organization, coordination, communication, operations, and training activities that result in a safe sporting event experience. This document is For Official Use Only (FOUO) and is available to vetted critical infrastructure owners and operators on request based on a demonstrated need to know. For more information, contact the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

Sector Annual Reports The Sector-Specific Agency Executive Management Office (SSA EMO) Collaborates with State, local, Tribal and territorial government and the private sector to develop, maintain and update Sector Annual Reports for the Chemical, Commercial Facilities, Critical Manufacturing, Dams, Emergency Services, and Nuclear Sectors. These reports are For Official Use Only (FOUO) and available to vetted private sector critical infrastructure owners and operators with a demonstrated need to know. For more information, contact ssaexecsec@dhs.gov.

Sector-Specific Agency Executive Management Office (SSA EMO) Sector Snapshots, Fact Sheets and Brochures These documents provide a quick look at SSA EMO sectors and generally contain sector overviews; information on sector partnerships; information on key CIKR protection issues and Priority Programs. The products bring awareness to CIKR issues and encourage sector participation in critical infrastructure protection risk management activities. These products include: fact sheets and brochures for the Chemical, Commercial Facilities, Critical Manufacturing, Dams, Emergency Services and Nuclear Sectors. Additional materials available on request. See http://www.dhs.gov/files/programs/gc_1189168948944.shtm. For more information, contact NIPP@dhs.gov.

Sector-Specific Pandemic Influenza Guides (Sector-Specific Agency Executive Management Office (SSA EMO) Sectors) SSA EMO worked with Partnership and Outreach Division to develop sector-specific guides for pandemic influenza for the Chemical, Commercial Facilities, Dams, Emergency Services, and Nuclear Sectors. Available on request by contacting SSAexecsec@dhs.gov.

Sector-Specific Plans detail the application of the National Infrastructure Protection Plan (NIPP) risk management framework to the unique characteristics and risk landscape of each sector. The SSPs provide the means by which the NIPP is implemented across all the critical infrastructure and key resources (CIKR) sectors. Each Sector-Specific Agency is responsible for developing and implementing an SSP through a coordinated effort involving their public and private sector CIKR partners. For publicly-available plans, please visit http://www.dhs.gov/files/programs/gc_1179866197607.shtm. For more information, contact NIPP@dhs.gov.

State and Local Implementation Snapshot The National Infrastructure Protection Plan (NIPP) provides the coordinated approach for establishing national priorities, goals, and requirements for critical infrastructure and key resources protection so that Federal funding and resources are applied in the most effective manner to reduce vulnerability, deter threats, and minimize the consequences of attacks and other incidents. This two-page snapshot describes the role of State and local governments in implementing the NIPP. This snapshot is available by contacting the NIPP Program Management Office at NIPP@dhs.gov.

Summary of the NIPP and SSPs provides the executive summary of the 2006 National Infrastructure Protection Plan (NIPP), as well as the executive summaries of each of the 17 supporting Sector-Specific Plans (SSPs). The 18th sector, Critical Manufacturing, is not included in this summary document. This document is available by contacting the NIPP Program Management Office at NIPP@dhs.gov.

Who's Who in Chemical Sector Security (October 2008) The document describes the roles and responsibilities of different DHS components with relation to Chemical Security. See http://training.fema.gov/EMIWeb/IS/IS860a/CIKR/assets/ChemicalSectorWhosWho.pdf. For more information, contact the Chemical Sector-Specific Agency at ChemicalSector@dhs.gov.

Who's Who in Emergency Services Sector describes the roles and responsibilities of the DHS components with relation to the Emergency Services Sector. Contact the Emergency Services Sector-Specific Agency ESSTeam@hq.dhs.gov.

IP Programs/Services/Events

Bomb-making Materials Awareness Program (BMAP) Developed in cooperation with the Federal Bureau of Investigation, BMAP is designed to assist local law enforcement agencies engage a wide spectrum of private sector establishments within their jurisdictions that manufacture, distribute, or sell products that contain home-made explosives (HMEs) precursor materials. BMAP outreach materials, provided by law enforcement to these local businesses, help employees identify HME precursor chemicals and other critical improvised explosive devices (IED) components of concern, such as electronics, and recognize suspicious purchasing behavior that could indicate bomb-making activity. To request materials or additional information, contact the DHS Office for Bombing Prevention at OBP@dhs.gov, (703) 235-5723.

Buffer Zone Protection Program (BZPP) is a DHS administered infrastructure protection grant program targeted to local law enforcement (LLE). The BZPP provides funding to LLE for equipment acquisition and planning activities to address gaps and enhance security capabilities. It is also designed to increase first responder capabilities and preparedness by bringing together private sector security personnel and first responders in a collaborative security planning process that enhances the buffer zone – the area outside a facility that can be used by an adversary to conduct surveillance or launch an attack, around individual assets. Detailed BZPP annual grant guidance is available on the DHS/FEMA grants web site (http://www.fema.gov/government/grant/bzpp/).

Cesium Chloride In-Device Delay (Irradiator Hardening) DHS, as the Nuclear Sector-Specific Agency, coordinates with Department of Energy's National Nuclear Security Administration (NNSA), which is collaborating with the private sector and other Federal agencies to enhance the security of blood and research irradiators that use cesium chloride sources (Cs-137). This effort includes the three major domestic manufacturers and vendors of self-contained irradiators containing Cs-137. The security enhancements consist of adding in-device delay (IDD) kit, which significantly increases the amount of time needed for the unauthorized removal of the radioactive material. The objective is to implement security enhancements that minimize impact to the user community. For more information, ontact the Nuclear Sector-Specific Agency at nuclearSSA@hq.dhs.gov.

Chemical Facility Anti-Terrorism Standards (CFATS) Chemical Facility Security Tip Line Individuals who would like to report a possible security concern involving the CFATS regulation at their facility or at another facility may contact the CFATS Chemical Facility Security Tip Line. They are welcome to report these concerns on the voicemail anonymously, or, if they would like a return call, they may leave their name and contact number. See www.dhs.gov/chemicalsecurity or Contact the CFATS Chemical Facility Security Tip Line at (877) FYI-4-DHS (1-877-394-4347). To report a potential security incident that has already occurred, call the National Infrastructure Coordination Center at (202) 282-9201.

Chemical Security Summit is an annual industry benchmark event, co-sponsored by DHS and the Chemical Sector Coordinating Council. See http://www.dhs.gov/files/programs/gc_1176736485793.shtm. For more information, contact the Chemical Sector-Specific Agency at 1-877-CHEMSEC, ChemicalSector@dhs.gov.

Chemical Security Compliance Assistance Visit (CAV) Requests Upon request, the Infrastructure Security Compliance Division (ISCD) provides Compliance Assistance Visits (CAV) to Chemical Facility Anti-Terrorism Standards (CFATS)-covered facilities. CAVs are designed to provide in-depth knowledge of and assistance in a facility's efforts to comply with CFATS. Those interested in a CAV can find more information about these visits at DHS' chemical security web site: www.dhs.gov/chemicalsecurity To request a CAV, contact cscd.ieb@hq.dhs.gov.

Chemical Sector Monthly Suspicious Activity Calls Employees of chemical companies, associations, and agencies who have a need to know information concerning potential physical and cyber threats and vulnerabilities to chemical infrastructure are eligible to listen in on the briefings. This monthly unclassified suspicious activity call for the Chemical Sector is scheduled for the first Wednesday of every month at 10:00AM EDT. The call-in information is as follows: DDI number: (800) 501-9384, Conference ID: 4754043. Contact the Chemical Sector-Specific Agency at ChemicalSector@dhs.gov.

Critical Infrastructure and Key Resource (CIKR) Asset Protection Technical Assistance Program (CAPTAP) assists State and local law enforcement, first responders, emergency management, and other homeland security officials understand the steps necessary to develop and implement a comprehensive CIKR protection program in their respective jurisdiction through the facilitated sharing of best practices and lessons learned. This includes understanding processes, methodologies, and resources necessary to identify, assess, prioritize, and protect CIKR assets, as well as those capabilities necessary to prevent and respond to incidents, should they occur. Through a partnership with the National Guard Bureau (NGB), the U.S. Army Research, Development and Engineering Command (RDECOM), and the DHS Office of Infrastructure Protection (IP) Infrastructure Information Collection Division (IICD), this service also provides Web-based and instructor-led training on Protected Critical Infrastructure Information (PCII) and the use of the *Automated Critical Asset Management System* (ACAMS) and *Integrated Common Analytical Viewer* (iCAV) system. See www.dhs.gov/files/programs/gc_1195679577314.shtm. For additional information, contact ACAMS-info@hq.dhs.gov, or (703) 235-3939.

Dams Sector Exercise Series (DSES) In collaboration with sector partners, including the Emergency Services SSA, the Dams SSA has developed an exercise series to test interoperability, preparedness, and regional resilience. DSES-09: Columbia River Basin was an effort undertaken in collaboration with the Pacific Northwest Economic Region, U.S. Army Corps of Engineers, and Pacific Northwest region stakeholders to conduct exercise series along the Columbia River Basin to develop an Integrated Regional Strategy to improve disaster resilience and preparedness for the Tri-Cities region of Washington State. See http://training.fema.gov/EMIWeb/IS/IS860a/CIKR/assets/2009DamsSectorExerciseSeries-ColumbiaRiverBasinFactSheet.pdf. For more information, contact the Dams Sector-Specific Agency at dams@dhs.gov.

Enhanced Critical Infrastructure Protection (ECIP) Visits are conducted by Protective Security Advisors (PSAs) in collaboration with Critical Infrastructure and Key Resources (CIKR) owners and operators to assess overall facility security and increase security awareness. ECIP Visits are augmented by the Infrastructure Survey Tool (IST), a web-based tool that provides the ability to collect, process, and analyze ECIP survey date in near real time. Data collected during an ECIP visit is consolidated in the IST and then weighted and valued, which enables the development of ECIP metrics; conduct sector-by-sector and cross-sector vulnerability comparisons; identify security gaps and trends across CIKR sectors and sub-sectors; and establish sector baseline security survey scores. Private sector owners and operators interested in receiving an ECIP Visit should contact the PSA Field Operations Staff PSAFieldOperationsStaff@hq.dhs.gov (703) 235-5724.

National Infrastructure Advisory Council (NIAC) provides the President through the Secretary of Homeland Security advice on the security of the critical infrastructure sectors and their information systems. The Council is composed of a maximum of 30 members, appointed by the President from private industry, academia, and State and local government. For more information, see www.dhs.gov/niac.

National Infrastructure Protection Plan (NIPP) Sector Partnership improves the protection and resilience of the nation's critical infrastructure. The partnership provides a forum for the designated 18 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/cipac or by contacting Sector.Partnership@dhs.gov.

Office of Infrastructure Protection (IP) and National Infrastructure Protection Plan (NIPP) booths are available for exhibiting 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 NIPP@dhs.gov.

Protected Critical Infrastructure Information (PCII) Program is an information sharing resource designed to facilitate the flow and exchange of critical infrastructure information (CII) between the private sector, DHS and Federal, State and local government entities. Private sector entities can voluntarily submit their CII to the PCII Program for use in Federal, State and local critical infrastructure protection efforts. Once the PCII Program has validated and marked the CII as PCII, the information will be safeguarded, disseminated and used in accordance with PCII requirements established pursuant to the Critical Infrastructure Information Act of 2002 and the implementing Regulation. PCII is protected from disclosure under Federal, State and local disclosure laws and from use in civil litigation and for regulatory purposes. Information about the PCII Program, including the CII Act of 2002, the implementing Regulation and the PCII Program Procedures Manual can be found on the Program's web site at www.dhs.gov/pcii. For additional information, contact pcii-info@dhs.gov, or (202) 360-3023.

Protective Security Advisor (PSA) Program Established in 2004, the PSA Program provides a locally-based DHS infrastructure security expert as the link between State, local, Tribal, territorial, and private sector organizations and DHS infrastructure protection resources. PSAs assist with ongoing State and local critical infrastructure and key resources (CIKR) security efforts, coordinate vulnerability assessments and training, support incident management, and serve as a vital channel of communication between private sector owners and operators of CIKR assets and DHS. Private sector owners and operators interested in contacting their PSA should contact the DHS Protective Security Advisor (PSA) Field Operations Staff: PSAFieldOperationsStaff@hq.dhs.gov or (703) 235-5724.

Radiological Voluntary Security Enhancements DHS, as the Nuclear Sector-Specific Agency, coordinates with security experts from the Department of Energy's national laboratories, led by National Nuclear Security Administration (NNSA) headquarters staff, to provide security assessments, share observations, and make recommendations for enhancing security at facilities which house high-risk radioactive sources. The security upgrades are aimed at improving deterrence, control, detection, delay, response, and sustainability. Contact the Nuclear Sector-Specific Agency at nuclearSSA@hq.dhs.gov.

Regional Resiliency Assessment Program (RRAP) is a cooperative DHS led interagency assessment of specific critical infrastructure and key resources (CIKR) and regional analysis of the surrounding infrastructure, including key interdependencies. The emphasis for the RRAP is infrastructure "clusters," regions, and systems. . The assessment and its final report are protected as Protected Critical Infrastructure Information (PCII). Regions are selected collaboratively by State and DHS Officials. Private sector CIKR owners and operators of infrastructure interested in receiving more information on the RRAP should contact the DHS Protective Security Advisor (PSA) Field Operations Staff: PSAFieldOperationsStaff@hq.dhs.gov or (703) 235-5724.

Research and Test Reactors (RTRs) Voluntary Security Enhancement Program As Chair of the Nuclear Government Coordinating Council (GCC) and a participant in the Joint GCC-Sector Coordinating Council (public-private) Research and Test Reactor (RTR) Subcouncil, the Nuclear Sector-Specific Agency coordinates with the Department of Energy's National Nuclear Security Administration on voluntary security enhancements at RTR facilities nationwide. Security enhancements are jointly determined by NNSA and the facility owner-operator and are funded by NNSA. These enhancements improve security beyond what is required by law and are consistent with RTR security regulations. For additional information, contact the Nuclear Sector-Specific Agency nuclearSSA@hq.dhs.gov.

Sector-Specific Agency Executive Management Office/Transportation Security Administration (TSA) Joint Exercise Programs Working with support and funding from TSA, this potentially multi-year program allows Critical Manufacturers with planning support by TSA's Intermodal Security Training and Exercise Program (ISTEP) to develop advanced table-top exercises that determine gaps and mitigate vulnerabilities in their respective transportation supply chains within the U.S. and cross border (particularly across Canadian and Mexican borders). For more information, contact the Critical Manufacturing Sector-Specific Agency cm-ssa@dhs.gov.

Security Outreach and Awareness Program (SOAP) provides critical information to chemical facility managers, control engineers, and IT administrators working in cyber-security management. Participating companies receive a free voluntary review of the security of their system networks and a summary of their cybersecurity policies and processes. For more information, contact the Chemical Sector-Specific Agency at ChemicalSector@dhs.gov.

Security Seminar Exercise Series with State Chemical Industry Councils This collaborative effort between the DHS Chemical Sector-Specific Agency and various state chemical industry councils fosters communication between facilities and their local emergency response teams by encouraging representatives to share their insight, knowledge, and experiences during a facilitated table-top exercise. The exercises can include a wide-variety of topics and are catered towards the specific interests of the local chemical facilities. For more information, contact the Chemical Sector-Specific Agency at ChemicalSector@dhs.gov.

Site Assistance Visit (SAV) is a facility vulnerability assessment focused on identifying security gaps and providing options for consideration to enhance protective measures. The SAV uses analyses of critical assets and current security measures, and scenario-based approaches such as assault planning to identify vulnerabilities and develop mitigation strategies. Following the assessment, DHS provides critical infrastructure and key resources (CIKR) owners and operators with an SAV Report,

protected as Protected Critical Infrastructure Information (PCII). The report details the facility information and offers options for consideration to increase the ability to detect and prevent terrorist attacks and reduce infrastructure vulnerabilities. Private sector owners and operators interested in receiving more information on the SAV should contact the DHS Protective Security Advisor (PSA) Field Operations Staff: PSAFieldOperationsStaff@hq.dhs.gov or (703) 235-5724.

IP Web-Based Resources

Automated Critical Asset Management System (ACAMS) is a secure, Web-based portal designed to help State and local emergency responders, such as infrastructure protection planners, homeland security officials, law enforcement personnel, and emergency managers, collect and organize critical infrastructure and key resource (CIKR) asset data as part of a comprehensive CIKR protection program. ACAMS is managed by the Office of Infrastructure Protection (IP) and continues to be developed in partnership with State and local communities. ACAMS benefits include it is provided at no cost for State and local use, it has public disclosure protections through the Protected Critical Infrastructure Information (PCII) program, and it is an integrated approach for collecting, protecting and analyzing CIKR asset data. The Federal Emergency Management Agency's National Preparedness Directorate also supports Critical Infrastructure Protection-related ACAMS training. See www.dhs.gov/ACAMS. For more information, contact ACAMS-info@hq.dhs.gov or (703) 235-3939.

Chemical Security Assessment Tool (CSAT) is an online tool developed by the Infrastructure Security Compliance Division (ISCD) to streamline the facility submittal and subsequent DHS analysis and interpretation of critical information used to 1) preliminarily determine facility risk, 2) assess high-risk facility's vulnerability 3) describe security measures at high risk sites and 4) ultimately track compliance with the CFATS program. CSAT is a secure information portal that includes applications for completing the User Registration, Top-Screen, Security Vulnerability Assessment (SVA), and Site Security Plan (SSP). ISCD provides user guides to assist with each of these applications. See http://www.dhs.gov/files/programs/gc_1169501486197.shtm. Contact the CFATS Help Desk at csat@dhs.gov, (866) 323-2957.

Computer Based Assessment Tool (CBAT) is a cross-platform tool that integrates 360 degree geospherical video, geospatial and aerial imagery of facilities, surrounding areas, routes, and other areas of interest with a wide variety of other facility data, including evacuation plans, vulnerability assessments, standard operating procedures, and schematic/floor plans. By integrating this disparate data, the CBAT provides a comprehensive visual guide of a site that assists facility owners and operators, local law enforcement, and emergency response personnel to prepare for and respond to an incident. This resource is protected at the Protected Critical Infrastructure (PCII) and For Official Use Only (FOUO) level and is available to vetted private sector critical infrastructure owners and operators with a demonstrated need to know. For more information, contact the DHS PSA Field Operations Staff: PSAFieldOperationsStaff@hq.dhs.gov or (703) 235-5724.

Critical Infrastructure and Key Resources (CIKR) Resource Center was designed to build awareness and understanding of each sector's scope and efforts to ensure CIKR protection and resiliency. The Center offers a centralized location page to find sector goals, plans, priorities, online training modules, activities and achievements, useful links, and other sector-based and cross sector resources. See http://training.fema.gov/emiweb/is/IS860a/CIKR/index.htm. For more information, contact IP_Education@hq.dhs.gov.

Dams Sector Consequence-Based Top Screen Methodology is an online tool based on the methodology developed to identify the subset of those high-consequence facilities whose failure or disruption could potentially lead to the most severe impacts. The Web-based tool was developed to support the implementation of the methodology across the sector. Available on LENS – https://lens.iac.anl.gov, for more information contact the Dams Sector-Specific Agency at dams@dhs.gov.

Dams Sector Suspicious Activity Reporting Tool is an online reporting tool within the Homeland Security Information Network-Critical Sectors Dams Portal that was established to provide sector stakeholders with the capability to report and retrieve information pertaining to suspicious activities that may potentially be associated with pre-incident surveillance, and those activities related to the exploration or targeting of a specific critical infrastructure facility or system. It is accompanied by a Fact Sheet/Brochure. For additional information, contact the Dams Sector-Specific Agency at dams@dhs.gov.

DHS 20-Minute Retail Security Webinar is a web-based application dealing with security issues for all shopping center, mall, and retail employees. The webinar, produced by the Office of Infrastructure Protection's Protective Security Coordination Division (Office for Bombing Prevention), covers issues such as overall security awareness, suspicious purchases and unattended or suspicious packages. To request, contact the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

DHS 90-Minute Retail Security Webinar is a web-based application similar to the 20-minute Retail Security Webinar but designed for mall and retail professional security staff. The webinar, produced by the Office of Infrastructure Protection's Protective Security Coordination Division (Office for Bombing Prevention), offers greater detail on the topics covered in the 20-minute webinar, but with a greater scope and detail. Available on request. For additional information, please contact the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

General Information on Sector-Specific Agency Executive Management Office (SSA EMO) Critical Infrastructure and Key Resources (CIKR) Sectors and Programs provides an overview of the SSA EMO mission in CIKR risk management, and a description of SSA EMO Sectors. See http://www.dhs.gov/xabout/structure/gc_1204058503863.shtm. Contact the Sector-Specific Agency Executive Management Office at SSAexecsec@dhs.gov).

Homeland Security Information Network-Critical Sectors (HSIN-CS) is the primary information-sharing platform between the Critical Infrastructure/Key Resource sector stakeholders. HSIN-CS enables DHS and critical infrastructure owners and operators to communicate,

coordinate, and share sensitive and sector-relevant information to protect their critical assets, systems, functions and networks, at no charge to sector stakeholders. Vetted critical infrastructure private sector owners and operators are eligible to access HSIN-CS. To request access to HSIN-CS, please e-mail CIKRISEAccess@hq.dhs.gov. When requesting access, please indicate the critical infrastructure sector to which your company belongs and include your name, company, official e-mail address, and supervisor's name and phone number.

Integrated Common Analytical Viewer (iCAV) provides a suite of free, Web-based, infrastructure-focused geospatial visualization and analysis tools managed by the DHS Office of Infrastructure Protection. The two primary tools in the iCAV suite are the iCAV Next Generation Web-based visualization and analysis platform and the DHS Earth data service, both of which provide authoritative infrastructure data and various dynamic situational awareness feeds in standard geographic information system (GIS) data formats to authorized Homeland Security Information Network (HSIN) users at the Federal, State, and local levels and within the private sector. iCAV Next Generation is also the GIS platform for the *Automated Critical Asset Management System* (ACAMS). See www.dhs.gov/icav. For more information, contact iCAV.info@hq.dhs.gov, or (703) 235-4949.

Risk Self-Assessment Tool (RSAT) for Stadiums and Arenas is a secure, Web-based application designed to assist managers of stadiums and arenas with the identification and management of security vulnerabilities to reduce risk to their facilities. The RSAT application uses facility input in combination with threat and consequence estimates to conduct a comprehensive risk assessment and provides users with options for consideration to improve the security posture of their facility. Accompanied by a Fact Sheet/Brochure. See http://www.dhs.gov/files/programs/gc_1259861625248.shtm. For additional information, please contact the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

Technical Resource for Incident Prevention (TRIP*wire*) (www.tripwire-dhs.net) is DHS's 24/7 online, collaborative, information-sharing network for bomb squad, law enforcement, and other first responders to learn about current terrorist improvised explosive device (IED) tactics, techniques, and procedures. The system combines expert analyses and reports with relevant documents, images, and videos gathered directly from terrorist sources to assist law enforcement anticipate, identify, and prevent IED incidents. To request additional information, contact DHS Office for Bombing Prevention at OBP@dhs.gov, (703) 235-5723.

TRIP*wire* Community Gateway (TWCG) is a TRIP*wire* web portal designed specifically for the Nation's CIKR owners, operators, and private security personnel. TWCG provides expert threat analyses, reports, and relevant planning documents to help key private sector partners anticipate, identify, and prevent improvised explosive device (IED) incidents. TWCG shares IED-related information tailored to each of the 18 CIKR Sectors as well as a Community Sector for educational institutions, in accordance with the National Infrastructure Protection Plan (NIPP). TWCG information is currently 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.. To request additional information, contact the DHS Office for Bombing Prevention at OBP@dhs.gov, (703) 235-5723.

Voluntary Chemical Assessment Tool (VCAT) is a secure, Web-based application that allows owners and operators to identify their facilities' current risk level using an all-hazards approach and facilitates a cost-benefit analysis by allowing them to select the best combination of physical security countermeasures and mitigation strategies to reduce overall risk. There is also a brochure that describes the features and benefits of VCAT and includes instructions on how to gain access to the tool. Accompanied by Fact Sheet/Brochure. Available on request. For more information, contact the Chemical Sector-Specific Agency at ChemicalSector@dhs.gov.

Science & Technology Directorate (S&T)

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

S&T Programs

S&T Collaboration in Data and Visual Analytics both internally within the DHS research community as well as externally enables S&T to leverage both its funding and technical expertise by taking advantage of research activities underway in government laboratories, industry laboratories, and in universities across the world. In 2008 S&T's Command, Control, and Interoperability Division (CCI) established a five-year joint program with the National Science Foundation (NSF) on the Foundations of Visual and Data Analytics. In 2009, CCI contributions were matched more than twofold by NSF, and 16 universities have been awarded research grants. Additionally, DHS has signed formal international collaboration agreements between Canada and Germany, and discussions with United Kingdom (UK) and France are underway. These efforts have resulted in the development of joint scientific and technical projects in visualization and data analytics. For more information, contact iVAC@dhs.gov.

Commercial Mobile Alert Service (CMAS) is a component of the Integrated Public Alert and Warning System. It is an alert system that will have the capability to deliver relevant, timely, effective, and targeted alert messages to the public through cell phones, blackberries, pagers, and other mobile devices. This national capability will ensure more people receive Presidential, Imminent Threat, and AMBER alerts. In support of this effort, the first CMAS Forum was recently held. The purpose of the Forum was to convene the alerts and warnings community-including message originators, emergency responder organizations, industry organizations, academia, and organizations representing special needs populations-to address critical issues and determine next steps for the CMAS Research, Development, Test and Evaluation (RDT&E) program. Action teams based around the initiatives that came out of the CMAS Forum were created and are being populated. http://www.cmasforum.com/, contact cmasforum@sra.com.

Commercialization Office is responsible for the development and implementation of a commercialization process and for the execution of two innovative public-private partnerships that leverage research and development efforts in the private sector that are aligned to detailed operational requirements from Department stakeholders. The Commercialization Office also spearheads DHS S&T's outreach efforts that inform the private sector on "How to do business with DHS." See http://www.dhs.gov/xabout/structure/gc_1234194479267.shtm. Contact: SandT_Commercialization@hq.dhs.gov, 1-(202) 254-6749.

Cyber Security Research and Development Center (CSRDC) S&T has the mission to conduct research, development, test and evaluation, and timely transition (RDTE&T) of cyber security capabilities to operational units within DHS, as well as Federal, State, local and critical infrastructure sector operational end-users for homeland security purposes. As part of its cyber security mission, DHS/S&T has established the Cyber Security Research and Development Center (CSRDC). As part of its cyber security mission, DHS/S&T utilizes CSRDC to focus cyber security RDTE&T efforts and to involve the best practices and personnel from academic, private industry and federal and national laboratories. The Cyber Security R&D Center was established by the Department of Homeland Security in 2004 to develop security technology for protection of the U.S. cyber infrastructure. For example, the Linking the Oil and Gas Industry to Improve Cyber Security (LOGIIC) project, which addresses security vulnerability issues related to the oil and gas industry's Process Control Systems (PCS) and Supervisory Control and Data Acquisition systems. The comprehensive monitoring system developed in LOGIIC provides an integrated, multi-component security solution that monitors a PCS for abnormal activity. The Center conducts its work through partnerships between government and private industry, the venture capital community, and the research community. The Center conducts its work through partnerships between government and private industry, the venture capital community, and the research community. This web site provides information about this and other DHS S&T projects, workshop information and presentations, cybersecurity news, events and outreach information. See http://www.cyber.st.dhs.gov/, contact csrdc@dhs.gov.

Defense Technology Experimental Research (DETER) The DETER testbed was jointly funded by S&T and the National Science Foundation (NSF) and has been open to the research community since March 2004. The centerpiece of the experimental environment is a safe (quarantined), but realistic, network testbed based on a mesh of clusters of homogeneous experimental nodes. DETER is a critical 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. Existing testing facilities cannot handle experiments on a large enough scale to represent today's operational networks or the portion of the Internet that might be involved in a security attack. Industry has only been able to test and validate new security technologies in small- to medium-scale private research laboratories that do not adequately simulate a real networking environment. Newsletters, published papers, videos and update presentations can be viewed at http://www.isi.edu/deter/. Contact testbed-ops@isi.deterlab.net.

Domain Name System Security Extensions (DNSSEC) Deployment Coordinating Initiative To strengthen the domain name system against attacks, S&T has initiated the DoDNSSEC Deployment Initiative. DNSSEC has been

developed to provide cryptographic support for domain name system (DNS) data integrity and authenticity. DHS sponsors a community-based, international effort to transition the current state of DNSSEC to large-scale global deployment, including sponsorship of the DNSSEC Deployment Working Group, a group of experts active in the development or deployment of DNSSEC. It is open for anyone interested in participation. The DNSSEC web site contains articles, published research papers, DNSSEC Tools, Case Studies, Workshop information and presentation materials. See http://www.dnssec-deployment.org/.

Emergency Data Exchange Language (EDXL) messaging standards help emergency responders exchange critical data, including alerts, hospital capacity, and availability of response personnel and equipment. Industry can leverage these standards to better ensure compliance and interoperability for their products. See http://www.oasis-open.org.

FutureTECH™ program targets critical research/innovation focus areas that detailed the long-term needs of the Department to partner with the private sector, university communities and national labs in the development of technology for future use by Department stakeholders**.** See http://www.dhs.gov/files/programs/gc_1242058794349.shtm. Contact SandT_Commercialization@hq.dhs.gov, (202) 254-6749.

Long Range Broad Agency Announcement (BAA) is a funding mechanism for original research that addresses DHS capability gaps, which are specified in Part I of its announcement under Research Areas of Strategic Interest. It also funds original research that advances the foundations of technical knowledge in the basic sciences. Successful submissions to the Long Range BAA 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?" All of S&T's divisions and special programs receive and evaluate submissions, as appropriate, through the Long Range BAA. For submission instructions, evaluation criteria, and to apply online, visit: https://baa.st.dhs.gov/.

National Science and Technology Council (NSTC) Subcommittee on Biometrics and Identity Management (BIdM) encourages greater collaboration and sharing of information on biometric activities among government departments and agencies; commercial entities; state, regional, and international organizations; and the general public. See www.Biometrics.gov, contact info@biometrics.org.

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 standards are focused on developing radios and other components that can interoperate regardless of manufacturer. P25 CAP allows emergency responders to confidently purchase and use P25-compliant products, and the Program represents a critical step toward allowing responders to communicate with their own equipment. In 2009, the first eight laboratories were officially recognized by DHS as part of the P25 CAP. A DHS-approved laboratory is authorized to produce test reports for P25 equipment. NPPD/CS&C/OEC coordinates the implementation of P-25 compliance standards with S&T to promote communications interoperability, and by encouraging grant recipients to purchase P-25 compliant equipment and technologies with Federal grant funding. See http://www.safecomprogram.gov/SAFECOM/currentprojects/project25cap/, contact P25CAP@dhs.gov.

The Protected Repository for the Defense of Infrastructure against Cyber Threats (PREDICT) will facilitate the accessibility of computer and network operational data for use in cyber defense research and development through large-scale research datasets. PREDICT allows partners to pursue technical solutions to protect the public and private information infrastructure. It also provides researchers and developers with real network data to validate their technology and products before deploying them online. This initiative represents an important three-way partnership between the federal government, critical information infrastructure providers, and the security development community (both academic and commercial). Within this project, the Los Angeles Network Data Exchange and Repository (LANDER), Network Traffic Data Repository to Develop Secure Information Technology Infrastructure, Routing Topology and Network Reliability Dataset Project, and Virtual Center for Network and Security Data serve as data set collectors and hosts. The PREDICT Data Coordinating Center helps manage and coordinate the research data repository. See https://www.predict.org, contact PREDICT-contact@rti.org.

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, within resource constraints, to provide long-term science and technology advances for the benefit of homeland security. The focus areas identified by S&T's Research Council, with input from our customers and the research community, summarize the fundamental work needed to support the future protection of our Nation. See http://www.dhs.gov/xabout/structure/gc_1242157296000.shtm. Contact the Director of Research, SandT.Research@dhs.gov , (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 operational requirements documents (ORDs) and a conservative estimate of the potential available market of Department stakeholders**.** See http://www.dhs.gov/files/programs/gc_1211996620526.shtm. Contact sandt_commercialization@hq.dhs.gov, (202) 254-6749.

Support Anti-Terrorism by Fostering Effective Technologies Act (SAFETY Act) is a program managed by the Office of SAFETY Act Implementation (OSAI). The program 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. As part of the

Homeland Security Act of 2002 (Public Law 107-296), 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. See www.SAFETYAct.gov. Contact SAFETYActHelpDesk@dhs.gov, (866) 788-9318.

Technologies for Critical Incident Preparedness (TCIP) Conference and Exposition TCIP highlights DOJ, DHS, and DoD technologies; RDT&E investments; and training tools for the emergency responder community. It provides a forum for emergency responders to discuss best practices and exchange information and offers a unique opportunity for emergency responders; business and industry; academia; and local, Tribal, State, and Federal stakeholders to network, exchange ideas, and address common critical incident technology, preparedness, response and recovery needs, protocols, and solutions. See http://www.tcipexpo.com.

DHS Technology Transfer Program serves as the focal point for technology transfer activities at the Department of Homeland Security. Currently, DHS operates from one centralized Office of Research and Technology Applications (ORTA) to manage technology transfers at each of its laboratories and throughout the Department. The 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 the DHS can have a tremendous potential for commercial applications throughout the nation and dramatically enhance the competitiveness of individual small businesses as well as expanding areas of exploration and cooperation for all non-federal partners. For more information, visit http://www.dhs.gov/xabout/structure/gc_1264538499667.shtm

Voice over Internet Protocol (VOIP) project researches IP-enabled communication technologies and evaluates promising solutions. This project will enable the emergency response community to confidently deploy and use IP technologies and integrate video, cellular, and satellite communications. In FY 2009, the project initiated testing and evaluation of IP solutions and completed the first VoIP profile as prioritized by the emergency response community. Ultimately, the project will complete the development of a set of standards based on the needs of emergency responders. DHS and the U.S. Department of Commerce (DOC) gathered key stakeholders from both the public safety and industry communities to form a working group. Led by the DHS Office for Interoperability and Compatibility and DOC's Public Safety Communications Research Program, the Public Safety VoIP Working Group works to define and clarify the expectations for VoIP in the public safety environment. See http://www.safecomprogram.gov/SAFECOM/currentprojects/voip/ and http://www.pscr.gov/projects/broadband/voip/voip.php, contact VoIP_Working_Group@sra.com.

Video Quality in Public Safety (VQiPS) As video technology has evolved, the array of options for public safety practitioners has grown and the interoperability challenges have become increasingly complex. Thus the need has emerged for public safety to collectively articulate their video quality needs to the manufacturing community. A VQiPS Working Group was formed to focus on the major policy, technology, and practical uses and challenges of public safety video systems. Comprised of emergency responders, academics, Federal partners, and vendors, the Working Group is currently creating an end-user guide to help practitioners articulate their needs to vendors when they look to purchase or upgrade video systems. See http://www.safecomprogram.gov/SAFECOM/currentprojects/videoquality/videoquality.htm and http://www.pscr.gov/projects/video_quality/video_about.php. Contact VQiPS_Working_Group@sra.com.

DHS Centers of Excellence

DHS Center of Excellence: Awareness & Location of Explosives-Related Threats (ALERT) develops new means and methods to protect the nation from explosives-related threats, focusing on detecting leave-behind Improvised Explosive Devices, enhancing aviation cargo security, providing next-generation baggage screening, detecting liquid explosives, and enhancing suspicious passenger identification. Resources include **Training Opportunities and courses in Explosives.** See http://www.northeastern.edu/alert/ and http://energetics.chm.uri.edu**.** For more information, contact universityprograms@dhs.gov.

DHS Center of Excellence: Preparedness and Catastrophic Event Response (PACER) optimizes our nation's preparedness in the event of a high-consequence natural or man-made disaster, as well as develops guidelines to best alleviate the effects of such an event. Resources available include a **Modeling & Simulation Catalog, a Model Memorandum of Understanding (MOU) between Hospitals during Declared Emergencies,** and the **Electronic Mass Casualty Assessment and Planning Scenarios Applet (EMCAPS)**. See http://www.pacercenter.org/. For more information, contact universityprograms@dhs.gov.

DHS Center of Excellence: National Center for Risk and Economic Analysis of Terrorism Events (CREATE) develops advanced tools to evaluate the risks, costs and consequences of terrorism, and guides economically viable investments in countermeasures that will make our Nation safer and more secure. Resources include: an **Executive Program for Counter-Terrorism, Aviation Safety & Security Program** covering the use of models and tools for evaluation of security and anti-terrorism, **Degree Specializations in Homeland Security Analysis,** and **the National Interstate Economic Model (NIEMO)** an operational multi-regional input-output economic impact model. See http://create.usc.edu/. For more information, contact universityprograms@dhs.gov.

DHS Center of Excellence: National Center for Food Protection and Defense (NCFPD) defends the safety and security of the food system from pre-farm inputs through consumption by establishing best practices, developing new tools and attracting new researchers to prevent, manage and respond to food contamination events. Resources include: **Food and Agriculture Criticality Assessment Tool (FAS-CAT); FoodSHIELD,** a web-based system for communication, coordination, community-building, education, and training among the nation's food and agriculture sectors; **Exercise Design and Facilitation; Event and Consequence Models; Continuous Tracking and**

Analyzing Consumer Confidence in the U.S. Food Supply Chain; Supply Chain Benchmarking Diagnostic Tool; Global Chronology of Incidents of Chemical, Biological, Radioactive and Nuclear Attacks from 1961-2005; Mass Production of Detection and Neutralizing Antibodies; Biosensors Courses; The Biosecurity Research Institute (BRI); The Frontier Program; Food Protection and Food Safety and Defense Graduate Certificate Programs; The National Agricultural Biosecurity Center (NABC); Optimized Detection of Intentional Contamination using Simulation Modeling; Risk Communication, Message Development/Evaluation and Training; decontamination protocols; and Regulatory, Policy, Technical, and Practical Issues related to Contaminated Food Disposal. For more information, see http://www.ncfpd.umn.edu/ or contact universityprograms@dhs.gov.

DHS Center of Excellence: National Center for Foreign Animal and Zoonotic Disease Defense (FAZD) protects against the introduction of high-consequence foreign animal and zoonotic diseases into the United States, with an emphasis on prevention, surveillance, intervention and recovery. Resources include **Courses on Foreign Animal and Zoonotic Diseases**, **Public and Private sector Awareness Materials**, **Field Guide to Handling Contaminated Animal and Plant Materials, Mass Livestock Carcass Management workshop, Specialists in Foreign Animal and Zoonotic Diseases, an Avian Influenza Study Curriculum, a Guide to Developing an Animal Issues Emergency Management Plan,** and a compilation of materials pertaining to the **Economic Impact of Foreign Animal Diseases to the United States.** See http://fazd.tamu.edu/. For more information, contact universityprograms@dhs.gov.

DHS Center of Excellence: National Center for Command, Control, and Interoperability (C2I) creates the scientific basis and enduring technologies needed to analyze massive amounts of information from multiple sources to more reliably detect threats to the security of the nation, its infrastructures and to the health and welfare of its populace. These new technologies will also improve the dissemination of both information and related technologies. Co-led by Purdue University and Rutgers University, available educational opportunities are geared towards educating the next generation of homeland security professionals with initiatives that span the entire career development pipeline, ranging from K-12 programs through undergraduate and graduate level work, to professional education and training. For more information, see http://www.purdue.edu/discoverypark/vaccine/ and http://www.ccicada.org/ or contact universityprograms@dhs.gov.

DHS Center of Excellence: Center for Maritime, Island, & Remote/Extreme Environment Security led by the University of Hawaii in Honolulu for maritime and island security and Stevens Institute of Technology in Hoboken, N.J., for port security, will strengthen maritime domain awareness and safeguard populations and properties unique to U.S. islands, ports, and remote and extreme environments. Programs include the **MARCOOS High Frequency Radar Network** and **the New York /New Jersey Harbor Maritime Awareness System**. See http://cimes.hawaii.edu/ and http://www.stevens.edu/csr/. For more information, contact universityprograms@dhs.gov.

DHS Center of Excellence: National Transportation Security Center of Excellence (NTSCOE) develops new technologies, tools and advanced methods to defend, protect and increase the resilience of the nation's multi-modal transportation infrastructure and education and training base lines for transportation security geared towards transit employees and professionals. Educational programs include **H1N1 Training for transit agency managers and employees**, **Educational opportunities in transportation** at the Mineta Transportation Institute (MTI), **Online Master of Science in Homeland Security Management degree** from the Homeland Security Management Institute of Long Island University. See http://www.cti.uconn.edu/, http://www.tougaloo.edu/, http://transportation.tsu.edu/NTSCE/home.htm, http://www.policy.rutgers.edu/centers/nti.php, http://www.southampton.liu.edu/homeland/index.html, http://transweb.sjsu.edu/, and http://www.mackblackwell.org/. For more information, contact universityprograms@dhs.gov.

DHS Center of Excellence: National Consortium for the Study of Terrorism and Responses to Terrorism (START) informs decisions on how to disrupt terrorists and terrorist groups, while strengthening the resilience of U.S. citizens to terrorist attacks. Resources include the **Minorities at Risk Organizational Behavior,** an open-source dataset covering political organizations representing the interests of ethnic groups whose political status and behavior is tracked by the Minorities at Risk project; the **Global Terrorism Database**, an open-source database including information on terrorist events around the world from 1970 through 2007; **Terrorist Organization Profiles;** and **Training Programs related to the Human Causes and Consequences of Terrorism**. See http://www.start.umd.edu/start/. For more information, contact universityprograms@dhs.gov.

Transportation Security Administration (TSA)

The Transportation Security Administration protects the Nation's transportation systems to ensure freedom of movement for people and commerce. www.tsa.gov

TSA Training and Education

Airport Watch/AOPA Training TSA partnered with the Aircraft Owners and Pilots Association (AOPA) to develop a nationwide Airport Watch Program that uses the more than 650,000 pilots as eyes and ears for observing and reporting suspicious activity. The Airport Watch Program includes warning signs for airports, informational literature, and a training video to teach pilots and airport employees how to enhance security at their airports. For additional information including a training video, visit http://www.aopa.org/airportwatch/.

Alien Flight/Flight School Training The Interim Final Rule, Flight Training for Aliens and Other Designated Individuals and Security Awareness Training for Flight School Employees, requires flight schools to ensure that each of its flight school employees who has direct contact with students (including flight instructors, ground instructors, chief instructors and administrative personnel who have direct contact with students) receive both initial and recurrent security awareness training. Flight schools may either choose to use TSA's security awareness training program or develop their own program. For more information, see http://www.tsa.gov/what_we_do/tsnm/general_aviation/flight_school_security.shtm.

First Observer ™ Training TSA provides funding for the First Observer ™ program under the Trucking Security Program grant. One component of First Observer is a security awareness training program. The First Observer ™ web site has online training modules for Trucking and School Bus with nine other modules planned. You can log on to the web site for training at: http://www.firstobserver.com/training/home.php. You can call (888) 217-5902 or E-mail (Firstobserver@hms-world.com) for more information.

Hazmat Motor Carrier Security Action Item Training (SAIT) Program addresses the TSA recommended security actions that were developed by the TSA for the hazmat transportation industry. For more information, see http://www.tsa.gov/highway. Or contact TSA Highway and Motor Carrier Division, highwaysecurity@dhs.gov.

Hazmat Motor Carrier Security Self-Assessment Training Program addresses the requirements contained in 49 Code of Federal Regulations (CFR), Part 172.802, which requires motor carriers that transport placarded amounts of hazardous materials to develop a plan that adequately addresses security risks related to the transportation of hazardous materials. Training materials can be found at http://www.tsa.gov/what_we_do/tsnm/highway/self_training.shtm. Contact TSA Highway and Motor Carrier Division with any questions at: highwaysecurity@dhs.gov.

IED Recognition and Detection for Railroad Industry Employees Training (CD) is a self-paced program that leads users through four separate modules which focus on heightening rail employees' awareness of suspicious activity. Topics covered include an overview of the terrorist threat, high risk targets, improvised explosive device recognition, and inspection and response procedures. See http://www.tsa.gov/what_we_do/tsnm/freight_rail/training.shtm, or contact freightrailsecurity@dhs.gov.

Intermodal Security Training and Exercise Program (I-STEP) supports TSA's Transportation Sector Network Management (TSNM) Modal Security Managers with exercises and training. The program is designed to support all transportation security partners with security objectives and training that has clear and consistent performance measures. See http://www.tsa.gov/what_we_do/layers/istep/index.shtm, contact i-step@dhs.gov, (571) 227-5150.

Land Transportation Antiterrorism Training Program (LTATP) is a joint effort by TSA and the Federal Law Enforcement Training Center (FLETC) to enhance knowledge, skills, and capabilities of law enforcement and security officials to prevent acts of terrorism. The program recognizes that security at most land transportation systems is accomplished by a cooperative effort of private sector and local, State, and federal government personnel. Through a curriculum focused on surface transportation security, this 5-day program provides the participants with tools to protect the land transportation infrastructure, including rail, mass transit and bus operations, and most importantly passengers and employees. See http://www.fletc.gov/training/programs/counterterrorism-division/land-transportation-antiterrorism-training-program-ltatp, contact: MassTransitSecurity@dhs.gov.

Maritime Passenger Security Courses TSA's Port & Intermodal Security Division creates and distributes training courses for passenger vessel employees. The courses address topics to improve passenger vessel employees' security awareness in their operating environments and to increase the effectiveness of their responses to suspicious items and persons that they might encounter. Courses available include: "Security Awareness For Passenger Vessel Employees," "IED/VBIED Recognition and Response," and "Crowd Control." To order, contact TSA Port & Intermodal Security Division at Maritime@dhs.gov, (571) 227-3556.

Mass Transit and Passenger Rail - Bomb Squad Response to Transportation Systems Through training and scenario-based exercises, this program expands regional capabilities to respond to a threat or incident involving a suspected explosive device in mass transit and passenger rail systems. Bomb technicians from law enforcement forces in the system's operating area are placed in the mass transit or passenger rail environment to confront exercise situations necessitating coordinated planning and execution of operations to identify, resolve, and, if appropriate, render harmless improvised explosive devices. These joint activities build relationships and skills

in a challenging operational setting, advancing operational partnerships that enhance capabilities to accomplish the prevention and response missions. Contact: MassTransitSecurity@dhs.gov.

Mass Transit and Passenger Rail - Field Operational Risk and Criticality Evaluation (FORCE) The purpose of this process is to establish a threat-based, risk-managed protocol that is particularly effective for regional use. This risk assessment evaluates threat, vulnerability, and consequence from a variety of vantage points, focusing primarily on the rail and bus properties but also surveying intermodal and interdependent critical infrastructure and key resources. The approach for any given region will apply the methodology that best addresses the needs of the particular transit agencies. The results of this assessment aid agencies in setting risk mitigation priorities and completing requests for grant awards and advance regional security collaboration. It is also adaptable to assist with new start-up properties about to come online or transit agencies with aggressive future expansion initiatives as well as regions hosting special security events. For more information, contact MassTransitSecurity@dhs.gov.

Mass Transit Smart Security Practices
In mass transit and passenger rail, TSA has produced a compilation of smart security practices drawn from the results of the comprehensive security assessments completed under the Baseline Assessment for Security Enhancement (BASE) program that evaluate agencies posture in the Security and Emergency Management Actions Items. TSA coordinated the preparation of this compilation with each agency with one or more practices recognized in a BASE assessment, ensuring an accurate description of the practice the agency developed and implemented and securing contact information for an official in the agency that professional colleagues may consult for more information. This compilation fosters communication among security professionals in mass transit and passenger rail nationally with the specific objective of expanding adoption of these most effective practices, tailored as necessary to each agency's operating environment. With the December 2009 update, the compilation now consists of some 80 smart security practices, many of which focus on regional partnerships, random security patrols, sweeps, and surges, and intelligence and security information sharing, and training and public awareness. For more information, please contact: MassTransitSecurity@dhs.gov.

Mass Transit Security Training Program Guidelines
Recognizing the vital importance of training frontline employees, TSA developed and implemented a focused security training initiative under the Transit Security Grant Program (TSGP) in February 2007. TSA coordinated development of this initiative through the Mass Transit SCC and the PAG. The resulting Mass Transit Security Training Program provides guidelines to mass transit and passenger rail agencies on the types of training to be provided by category of employee. The guidance further identifies specific courses developed under Federal auspices through the FTA, the Federal Emergency Management Agency, and TSA that are available to ensure employees are trained in the designated areas. Finally, the Department revised the eligible costs under the TSGP to allow coverage of overtime expenses incurred when employees receive training courses. For Mass Transit Security Training Program Guidelines, see http://www.tsa.gov/assets/pdf/TSGP_Training_IB243.pdf, for TSGP – Approved Training Programs List see http://www.tsa.gov/assets/pdf/approved_vendor_list.pdf. MassTransitSecurity@dhs.gov.

Operation Secure Transport (OST) is security awareness training for the Over-the-Road Bus industry. The training program will be available on CD and online. The training modules will be broken down into the following categories: Driver; Maintenance; Terminal Employees; Management; and Crisis Response. OST will have a link on the TSA Highway and Motor Carrier webpage in the near future: www.tsa.gov/highway. Contact TSA HMC with any questions at: highwaysecurity@dhs.gov.

Pipeline Security Awareness for the Pipeline Industry Employee Training CD and Brochures is a compact disc-based security awareness training program. The training is intended for distribution to interested pipeline companies and is centered on heightening pipeline employees' awareness of suspicious activity and their importance in keeping our nation's pipeline system secure. The training is useful to all pipeline company employees – administrative, operations, and security personnel – who need a basic level of awareness and understanding of pipeline security. To further enhance the information contained in the pipeline security awareness training CD, TSA produced the brochures "Pipeline Security Awareness for Employees" and "Good Neighbors! A Pipeline Security Neighborhood Watch." The CD and brochures may be requested on the TSA Pipeline Security web site at http://www.tsa.gov/what_we_do/tsnm/pipelines/training.shtm. For more information contact the Pipeline Security Division at PipelineSecurity@dhs.gov.

Public Transportation Emergency Preparedness Workshop - Connecting Communities Program brings mass transit and passenger rail agencies' security and emergency management officials together with Federal, State, local, and tribal government representatives and the local law enforcement and first responder community to discuss security prevention and response efforts and ways to work together more effectively to prepare and protect their communities. The 2-day Workshops enable the participants to apply their knowledge and experiences to a range of security and emergency response scenarios. The overall purpose is to foster dialogue, advance cooperative planning efforts, review past experiences, analyze best practices, and improve overall interoperability, resource utilization, and prevention and response capabilities to address threats, security incidents, and natural disasters. See http://www.connectingcommunities.net, contact: MassTransitSecurity@dhs.gov.

School Transportation Security Awareness (STSA) was developed by TSA in conjunction with the National Association of State Directors of Pupil Transportation Services, the National Association of Pupil Transportation and the National School Transportation Association to provide much needed security awareness information and training to the school transportation industry. STSA focuses on terrorist and criminal threats to school buses, bus passengers and destination facilities. It is designed to provide school bus drivers, administrators, and staff members with information that will enable them to effectively identify and report perceived security threats, as well as the skills to appropriately react and respond to a security incident should it occur. See

http://www.tsa.gov/what_we_do/tsnm/highway/stsa.shtm, contact highwaysecurity@dhs.gov.

TSA Publications and Guidance

Federal Bureau of Investigation (FBI) Terrorism Vulnerability Self-Assessment (Appendix B of the FTA SEPP guide – page 139 to 147). See http://transit-safety.volpe.dot.gov/publications/security/PlanningGuide.pdf. Contact the TSA Highway and Motor Carrier offices with any questions at: highwaysecurity@dhs.gov.

Federal Motor Carrier Safety Administration: Guide to Developing an Effective Security Plan for the Highway Transportation of Hazardous Materials See http://www.fmcsa.dot.gov/safety-security/hazmat/security-plan-guide.htm. Contact the TSA Highway and Motor Carrier offices with any questions at: highwaysecurity@dhs.gov.

General Aviation Security Guidelines In April 2003, TSA requested the Aviation Security Advisory Committee (ASAC) establish a Working Group made up of industry stakeholders to develop guidelines for security enhancements at the nation's privately and publicly owned and operated general aviation (GA) landing facilities. The resulting document constitutes a set of federally endorsed guidelines for enhancing airport security at GA facilities throughout the nation. It is intended to provide GA airport owners, operators, and users with guidelines and recommendations that address aviation security concepts, technology, and enhancements. For more information, visit: http://www.tsa.gov/what_we_do/tsnm/general_aviation/airport_security_guidelines.shtm

Keep the Nation's Railroad Secure (Brochure) assists railroad employees to recognize signs of a potential terrorist act. It is to be used in conjunction with a railroad company's existing security policies and procedures and may be modified to display the company's emergency contact information for ease of reference. See http://www.tsa.gov/what_we_do/tsnm/freight_rail/training.shtm or contact freightrailsecurity@dhs.gov.

Laminated Security Awareness Driver Tip Card contains the following topics: Bus Operator Alerts; Hijacking; Evacuating the Vehicle; Awareness and What to Look For; and Possible Chemical/Biological Weapons. See http://www.tsa.gov/what_we_do/tsnm/highway/documents_reports.shtm. Any questions can be sent to highwaysecurity@dhs.gov.

HAZMAT TRUCKING GUIDANCE: Highway Security-Sensitive Materials (HSSM) Security Action Items (SAIs) See http://www.tsa.gov/what_we_do/tsnm/highway/hssm_sai.shtm. Contact the TSA Highway and Motor Carrier offices with any questions at: highwaysecurity@dhs.gov.

Highway and Motor Carrier Awareness Posters include Motorcoach Awareness Posters for terminals: "Watch for Suspicious Items" and "Watch for Suspicious Behaviors" for terminals as well as a School Transportation Employee Awareness poster. See http://www.tsa.gov/what_we_do/tsnm/highway/documents_reports.shtm. Any questions can be sent to highwaysecurity@dhs.gov.

Mass Transit Employee Vigilance Campaign The "NOT ON MY SHIFT" program employs professionally-designed posters to emphasize the essential role that mass transit and passenger rail employees play in security and terrorism prevention in their systems. Adaptable templates enable each transit agency to tailor the product to its operations by including the system's logo, photographs of their own agency's employees at work, and quotes from the senior leadership, law enforcement and security officials, or frontline employees. The personalized approach has proven effective in gaining employees' attention and interest, supporting the participating transit and rail agencies' efforts to maintain vigilance for indicators of terrorist activity. TSA designs the posters based on the preferences of the particular mass transit or passenger rail agency. For more information contact: MassTransitSecurity@dhs.gov.

Mass Transit and Passenger Rail - Additional Guidance on Background Checks, Redress and Immigration Status The additional guidance on background checks, redress and immigration status supplement item 14 of the Security and Emergency Management Action Items, which recommends that the operators of mass transit conduct background investigations, such as criminal history and motor vehicle records, on all new frontline operations and maintenance employees and those employees and contractors with access to sensitive security information and security critical facilities and systems. This guidance addresses factors to consider on the recommended scope of and procedures for voluntarily conducted background checks. See http://www.tsa.gov/assets/pdf/guidance_employee_background_checks.pdf, contact: MassTransitSecurity@dhs.gov.

MOTORCOACH GUIDANCE: Security and Emergency Preparedness Plan (SEPP) See http://www.tsa.gov/assets/doc/sepp.doc. Contact the TSA HMC offices with any questions at: highwaysecurity@dhs.gov.

Rail Security Rule Overview On November 26, 2008 the Department of Homeland Security published a regulation governing security in the freight rail industry. The regulation not only affects freight railroads, but their customers as well. This presentation provides a high-level overview of the Rail Security Rule and information regarding the requirements of the regulation. See http://www.tsa.gov/assets/pdf/rail_rule_overview_for_stakeholder_workshops_mar_09.pdf (pdf – 229 KB), for more information contact: Scott.Gorton@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 is intended to assist 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.

Pipeline and Hazardous Materials Safety Administration: Risk Management Self-Evaluation Framework (RMSEF) See http://www.phmsa.dot.gov/hazmat/risk/rmsef.

Contact the TSA HMC offices with any questions at: highwaysecurity@dhs.gov.

Recommended General Aviation Security Action Items for General Aviation Aircraft Operators" and "Recommended Security Action Items for Fixed Base Operators". These voluntary action items are measures that aircraft operators and fixed base operators should consider when they develop, implement or revise security plans or other efforts to enhance security. For more information, see http://www.tsa.gov/what_we_do/tsnm/general_aviation/security.shtm.

Safeguarding America's Transportation System Security Guides are available for Highway Passenger Security Motorcoach Personnel, Private and Contract Carrier Company Employees, Owner-Operator Independent Drivers Association (OOIDA) Members, School Transportation Industry Personnel, Tank Truck Carrier Employees, and Truck Rental Company Employees. You can access the guides by clicking on "Documents and Reports" on the main Highway and Motor Carrier page on the TSA web site at: www.tsa.gov/highway. Any questions can be sent to highwaysecurity@dhs.gov.

Transportation Security Administration Counterterrorism Guides are highway security counterterrorism guides for Highway Transportation security partners in the Trucking, Highway Infrastructure, Motorcoach and School Transportation industries. These guides are small flip-charts containing the following topics: Pre-Incident Indicators; Targets; Threats to Highway; Insider Threat; Cloned Vehicle; Hijacking Prevention; Suspicious Packages; Information on Explosive Devices; Prevention/Mitigation; Security Planning; Security Inspection Checklist; Security Exercises; Chemical/Biological/Nuclear/Radiological Incidents; and Federal, State and Local POCs. You can contact TSA HMC to order a copy, pending available inventory at highwaysecurity@dhs.gov.

Transportation Sector Network Management Highway and Motor Carrier Division Annual Report TSA Highway and Motor Carrier Division publishes an Annual Report and posts the document on the following web site: http://www.tsa.gov/what_we_do/tsnm/highway/documents_reports.shtm.

Transit Agency Security and Emergency Management Protective Measures is a compilation of recommended protective measures for threat levels under the Homeland Security Advisory System Jointly developed by TSA and FTA. The current recommended protective measures reflect the advantages of improved threat and intelligence information, security assessments conducted by FTA and TSA, operational experience since the 9/11 attacks that prompted the original version, and collective subject matter expertise and experience of Federal partners and the transit community. This product has been developed as a technical resource to transit agency executive management and senior staff assigned to develop security and emergency response plans and to implement protective measures for response to the HSAS threat conditions and emergencies that might affect a transit agency. See http://www.tsa.gov/assets/pdf/mass_transit_protective_measures.pdf, contact: MassTransitSecurity@dhs.gov.

User's Guide on Security Seals for Domestic Cargo provides information on the different types of security seals available for use in securing and controlling containers, doors, and equipment. While this guide is not intended as a precise procedure for developing a comprehensive seal control program, instead, the objective is to provide information and procedures that will support the development of a seal control program that will meet site-specific requirements. The 'User's Guide on Security Seals' document can be obtained by accessing this link: https://portal.navfac.navy.mil/portal/page/portal/NAVFAC/NAVFAC_WW_PP/NAVFAC_NFESC_PP/LOCKS/PDF_FILES/sealguid.pdf.

TSA Alerts and newsletters

Highway ISAC The TSA Trucking Security Program funds the First Observer ™ domain awareness program as well as a Call-Center and Information Sharing and Analysis Center (ISAC). The Highway ISAC creates products and bulletins and e-mails them to a distribution list from TSA Highway and Motor Carrier and the First Observer program. Contact First Observer at www.firstobserver.com.

TSA Alert System is an emergency notification alert system for Highway and Motor Carrier security partners. The system is capable of sending out a message via phone, e-mail or SMS (text) based on the person's priority contact preference. Contact TSA by E-mail to become a TSA Alert subscriber at highwaysecurity@dhs.gov.

TSA Technical assistance and help

Comprehensive Security Assessments and Action Items encompass activities and measures that are critical to an effective security program. The 17 Action Items cover a range of areas including security program management and accountability, security and emergency response training, drills and exercises, public awareness, protective measures for the Homeland Security Advisory System threat levels, physical security, personnel security, and information sharing and security. TSA's Transportation Security Inspectors-Surface conduct security assessments under the Baseline Assessment for Security Enhancement (BASE) program that evaluate the posture of mass transit and passenger rail agencies in the Action Items in a comprehensive and systematic approach to elevate baseline security posture and enhance security program management and implementation. The results of the security assessments inform development of risk mitigation programs and resource allocations, most notably security grants. See http://www.tsa.gov/assets/pdf/mass_transit_action_items.pdf. For additional information, contact MassTransitSecurity@dhs.gov.

General Aviation Secure Hotline serves as a centralized reporting system for general aviation pilots, airport operators, and maintenance technicians wishing to report suspicious activity at their airfield. Hotline phone number: 1-866-GA-SECUR (1-866- 427-3287).

Highway and Motor Carrier First Observer ™ Call-Center "First Observer" trained specialists serve as the first line of communication for all matters related to this anti-terrorism and security awareness program. Well trained responders will provide nationwide first responder and

law enforcement contact numbers and electronic linkage to registered participants. Reported caller information is entered into a fully secured reporting system that allows for an electronic transfer to the Information Sharing and Analysis Center (ISAC) for further investigation by industry analysts. The call center may also be utilized during an incident of national significance. Call the center 24 x 7 (888) 217-5902. For more information see www.firstobserver.com.

Traveler Redress Inquiry Program (DHS TRIP) provides a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at airports,train stations, or crossing U.S. borders. To initiate an inquiry, please log onto DHS TRIP's interactive Web site www.dhs.gov/trip. For more information, contact the TSA Contact Center, (866) 289-9673.

TSA Programs and Services

Air Cargo Watch program The likelihood that office staff or managers will uncover the next terrorist is not high. The likelihood that an employee or contractor will see something that is out of the normal routine, the odd out of place person, activity or thing, is high. If it makes that employee feel uncomfortable or take notice, it should be reported to their supervisor immediately. The chance that a driver, dockworker, or cargo agent will be the person that uncovers the next attack is very likely. The Air Cargo Watch program involves all aspects of the supply chain reporting suspicious activity. TSA is collaborating with industry partners to increase security domain awareness so that individuals are empowered to detect, deter, and report potential or actual security threats. The resulting Air Cargo Watch campaign is consistent with U.S. Department of Homeland Security and TSA efforts. Air Cargo Watch has developed materials including a presentation, posters and a two-page guide, to encourage increased attention to potential security threats among several audiences. TSA encourages the display of posters and guides in public view to better attain its goal of maximizing security awareness along the entire air cargo supply chain. See http://www.tsa.gov/what_we_do/layers/aircargo/watch.shtm.

Cargo Certified Cargo Screening Program Effective August 1, 2010, 100 percent of cargo flown on passenger aircraft originating in the United States must be screened, per an act passed by Congress and signed into law by former President Bush following the 9/11 Commission Act of 2007. In response, TSA created the Certified Cargo Screening Program (CCSP) to provide a mechanism by which industry may achieve 100% screening without impeding the flow of commerce. Informational materials include: One-page overview of CCSP, CCSF and Chain of Custody Standards, Tri-Fold Brochure, Supplemental CCSP program material with at a glance program overview of the program Quick Hits overview with impact of 100% screening and supplemental CCSP materials. For more information visit: www.tsa.gov/ccsp, contact CCSP, ccsp@dhs.gov or the TSA Contact Center, (866) 289-9673.

Airspace Waivers The Office of Airspace Waivers manages the process and assists with the review of general aviation aircraft operators who request to enter areas of restricted airspace. For each waiver applicant, to support the vetting requirements, last name, first name, social security number, passport number, date of birth and place of birth, are collected. For applications for aircraft operating into, out of, within or overflying the United States, the waiver review process includes an evaluation of the aircraft, crew, passengers, and purpose of flight. The office then adjudicates the application and provides a recommendation of approval or denial to the FAA System Operations Security. For more information, see http://www.tsa.gov/what_we_do/tsnm/general_aviation/programs_aw.shtm#overview or contact (571) 227-2071.

DCA Access Standard Security Program (DASSP) TSA's Interim Final Rule, which was developed in coordination with other Department of Homeland Security agencies and the Department of Defense, takes into consideration the special security needs of Washington Reagan National Airport (DCA). Under TSA's security plan, a maximum of 48 flights in and out of DCA will be allowed each day. All aircraft will be required to meet the security measures set forth in the DCA Access Standard Security Program (DASSP). See http://www.tsa.gov/what_we_do/tsnm/general_aviation/programs_sp.shtm#dassp or contact (571) 227-2071.

General Aviation Maryland Three Program allows properly vetted private pilots to fly to, from, or between the three general aviation airports closest to the National Capital Region. These airports are collectively known as the "Maryland Three" airports, and include College Park Airport (CGS), Potomac Airfield (VKX) and Hyde Executive Field (W32.) These airports are all within the Washington, DC Air Defense Identification Zone (ADIZ) and the Washington, D.C. Flight Restricted Zone (FRZ). See http://www.tsa.gov/what_we_do/tsnm/general_aviation/programs_sp.shtm#maryland or contact (571) 227-2071

Homeland Security Information Network (HSIN) – Freight Rail Portal has been designed to provide consistent, real time information sharing capabilities in an integrated, *secure*, web-based forum to coordinate and collaborate directly with our security partners. Membership to the Freight Rail portal is provided once vetted by portal administrators. If you have questions, or for access please contact the HSIN Helpdesk at (866) 430-0162 or send an e-mail to HSIN.helpdesk@dhs.gov or Linda.Lentini@dhs.gov.

Homeland Security Information Network (HSIN) - Highway and Motor Carrier Portal is part of the Critical Sector part of the HSIN system (HSIN-CS). Membership to the HMC portal is provided once vetted by portal administrators. If you have questions, please contact the HSIN Helpdesk at (866) 430-0162 or send an e-mail to HSIN.helpdesk@dhs.gov.

Homeland Security Information Network – Public Transit Portal (HSIN-PT) Intelligence sharing between mass transit and passenger rail agencies and their Federal, State and local partners is further facilitated through TSA's Mass Transit Security Information Network's inter-agency communication and information sharing protocols. The HSIN-PT has been integrated into this network to provide one stop security information sources and outlets for security advisories, alerts and notices. TSA periodically produces and disseminates Mass Transit Security Awareness Messages that address developments related to terrorist activity and tactics against mass transit and passenger rail at the "for official use only" level. Additionally, TSA is actively involved in regional security forums and supports these collaborative efforts by sharing

intelligence products and related security information. Finally, a preplanned alert notification system enables access to mass transit and passenger rail law enforcement and security officials nationally with timely notification of threats or developing security concerns. Membership to the Public Transit portal is provided once vetted by portal administrators, contact MassTransitSecurity@dhs.gov.

Joint DHS/FBI Classified Threat and Analysis Presentations A joint DHS Office of Intelligence and Analysis, TSA Office of Intelligence, and Federal Bureau of Investigation effort provides classified intelligence and analysis presentations to mass transit and passenger rail security directors and law enforcement chiefs in more than 20 metropolitan areas simultaneously through the Joint Terrorism Task Force (JTTF) network's secure video teleconferencing system. These briefings advance two key strategic objectives - providing intelligence and security information directly to mass transit and passenger rail law enforcement chiefs and security directors and enhancing regional collaboration by bringing these officials together with their Federal partners to discuss the implications for their areas and coordinate to implement effective security solutions. The briefings occur on approximately quarterly to semi-annual basis, with additional sessions as threat developments may warrant. For more information, contact MassTransitSecurity@dhs.gov.

Mass Transit Security and Safety Roundtables TSA, The Federal Transit Administration (FTA), and the Federal Emergency Management Administration (FEMA) co-sponsor the semi-annual Transit Security and Safety Roundtables, bringing together law enforcement chiefs, security directors, and safety directors from the nation's 50 largest mass transit and passenger rail agencies and Amtrak with Federal security partners to discuss specific terrorism prevention and response challenges and to work collaboratively in developing effective risk mitigation and security enhancement solutions. The Roundtables also provide a forum for agency safety and security officials to share effective practices and develop relationships to improve coordination and collaboration. For additional information, contact MassTransitSecurity@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. Contact: MassTransitSecurity@dhs.gov.

Paperless Boarding Pass Pilot enables passengers to download their boarding pass on their cell phones or personal digital assistants (PDAs). This innovative approach streamlines the customer experience while heightening the ability to detect fraudulent boarding passes. For more information, see http://www.tsa.gov/approach/tech/paperless_boarding_pass_expansion.shtm or contact the TSA Contact Center, (866) 289-9673.

Screening Partnership Program (SPP) also known as Opt-Out, is a unique approach to providing security screening services for air passengers and baggage. Under the program, an airport operator may apply to have security screening conducted by personnel from a qualified private contractor working under Federal oversight. For more information, see http://www.tsa.gov/what_we_do/optout/index.shtm or contact the TSA Contact Center, (866) 289-9673.

Secure Fixed Base Operator is a public-private sector partnership program that allows Fixed Base Operators (FBOs) to check passenger and crew identification against manifests or Electronic Advance Passenger Information System (eAPIS) filings for positive identification of passengers and crew onboard general aviation aircraft. See http://www.tsa.gov/assets/pdf/sfbop_general_faq.pdf (pdf - 35KB). For additional information, contact tsnmfbo@dhs.gov.

Secure Flight is a behind the scenes program that enhances the security of domestic and international commercial air travel through the use of improved watch list matching. By collecting additional passenger data, it will improve the travel experience for all airline passengers, including those who have been misidentified in the past. Resources available for aviation stakeholders include a communications toolkit, a brochure, privacy information, signage informational video. For more information, visit http://www.tsa.gov/what_we_do/layers/secureflight/index.shtm, or contact the TSA Contact Center, (866) 289-9673.

Transportation Security Grant Programs provides security grants to transit systems, intercity bus companies, freight railroad carriers, ferries, and the trucking industry to help protect the public and the nation's critical transportation infrastructure. The grants support high-impact security projects that have a high efficacy in reducing the most risk to our nation's transportation systems. See www.tsa.gov/grants. For more information, contact TSAGrants@tsa.dhs.gov.

Transportation Worker Identification Credential (TWIC) is a security program designed to ensure that individuals who pose a security threat do not gain unescorted access to secure areas of the nation's maritime transportation system. The credential is a biometric card that ensures only vetted workers can enter without an escort to secure transportation areas. The TWIC Program is jointly administered by TSA and the U.S. Coast Guard. More information can be found at http://www.tsa.gov/what_we_do/layers/twic/index.shtm, or by contacting the TWIC Hotline, (866) 347-8942.

3-1-1 Liquid Restriction is a travel tip for passengers to remind them to pack liquids/gels in 3.4 oz bottles or less, to consolidate bottles into a one quart baggie and place them in a bin, outside of their carry-on to send through the X-ray for screening. See http://www.tsa.gov/311/index.shtm or contact the TSA Contact Center, (866) 289-9673.

Appendix A – Key Contacts

Component	Contact	E-mail	Phone
CBP	ACE Help Desk		(800) 927-8729
CBP	Air & Marine Operations Center (AMOC)		(951) 656-8000
CBP	Carrier Liaison Program	CLP@dhs.gov	(202) 344-3440.
CBP	CBP INFO Center		(877) CBP-5511
CBP	Client Representative Office		(571) 468-5000
CBP	Electronic System for Travel Authorization (ESTA)		(202) 344-3710
CBP	Global Entry	cbp.goes.support@dhs.gov	(866) 530-4172
CBP	Industry Partnership Program	industry.partnership@dhs.gov	(202) 344-1180
CBP	Intellectual Property Rights Help Desk	ipr.helpdesk@dhs.gov	(562) 980-3119 ext. 252
CBP	Intellectual Property Rights Policy and Programs	iprpolicyprograms@dhs.gov	
CBP	National Gang Intelligence Center		(703) 414-8600
CBP	Private Aircraft Travel Entry Programs	Private.Aircraft.Support@dhs.gov	
CBP	Secure Freight Initiative	securefreightinitiative@dhs.gov	
CRCL	Training	crcltraining@dhs.gov	(202) 357-8258
CRCL	Disability Preparedness	Disability.preparedness@dhs.gov	(202) 357-8483
CS&C	Control Systems Security Program (CSSP)	CSSP@dhs.gov	
CS&C	Cybersecurity Evaluation Tool	CSET@dhs.gov	
CS&C	Information Techhnology Sector	ncsd_cipcs@hq.dhs.gov	
CS&C	Office of Emergency Communications	oec@hq.dhs.gov	
CS&C	Software Assurance Program	software.assurance@dhs.gov	
CS&C	U.S. Computer Emergency Readiness Team (US-CERT)	info@us-cert.gov	(888) 282-0870
CS&C	US-CERT Secure Operations Center	soc@us-cert.gov	(888) 282-0870
DHS	Center for Faith-based and Community Initiatives	Infofbci@dhs.gov.	
DHS	Homeland Security Information Network (HSIN)	hsin.helpdesk@dhs.gov	(866) 430-0162
DHS	Lessons Learned and information Sharing (LLIS)	feedback@llis.dhs.gov	(866) 276-7001
DHS	National Information Exchange Model (NIEM) Program	NIEMPMO@NIEM.gov	
DHS	Office of Small and Disadvantaged Business Utilization		(202) 447-5555

DHS	Private Sector Office	Private.sector@dhs.gov	(202) 282-8484
FEMA	Center for Domestic Preparedness	Studentservices@cdpemail.dhs.gov	(866) 213-9553
FEMA	Centralized Scheduling and Information Desk	askcsid@dhs.gov	(800) 368-6498
FEMA	Citizen Corps	citizencorps@dhs.gov	
FEMA	Community Emergency Response Teams	cert@dhs.gov	
FEMA	Disaster Assistance		(800) 745-0243
FEMA	Emergency Lodging Assistance Program	femahousing@corplodging.com	(866) 545-9865
FEMA	FEMA Emergency Management Institute		(301) 447-1200
FEMA	FEMA Learning Resource Center	netclrc@dhs.gov	(800) 638-1821
FEMA	FEMA Private Sector Division	FEMA-Private-Sector-Web@dhs.gov	
FEMA	First Responder Training	askCSID@dhs.gov	(800) 368-6498
FEMA	Industry Liaison Support Center (contracting)		(202) 646-1895
FEMA	Maps Assistance Center	FEMAMapSpecialist@riskmapcds.com	(877) 336-2627
FEMA	National Incident Management System	FEMA-NIMS@dhs.gov	(202) 646-3850
FEMA	Regulations	FEMA-RULES@dhs.gov	
FEMA	Small Business Program	FEMA-SB@dhs.gov	
FEMA	Technical Assistance Program	FEMA-TARequest@fema.gov	(800) 368-6498
FEMA	U.S. Fire Administration		(301) 447-1000
FEMA	U.S. Fire Administration Publications	usfa-publications@dhs.gov	(800) 561-3356
FLETC	CRADA Program Office	FLETC-CRADAProgramOffice@dhs.gov	(912) 267-2100
I&A	DHS Open Source Enterprise	OSINTBranchMailbox@hq.dhs.gov	
I&A	Office of Intelligence and Analysis Private Sector Partnership Program	I&APrivateSectorCoordinator@hq.dhs.gov	(202) 447-3517 or (202) 870-6087
ICE	Victim Assistance Program		(866) 872-4973
ICE	Human Rights Violators and War Crimes Center	HRV.ICE@DHS.GOV	
ICE	ICE 24/7 Hotline		(866) DHS-2-ICE
ICE	ICE Mutual Agreement between Government and Employers Program (IMAGE)	IMAGE@dhs.gov	(202) 732-3064.
ICE	Intellectual Property Rights Center		(866) IPR-2060 or (866) 477-2060
ICE	National Incident Response Unit (NIRU)	niru@dhs.gov	
ICE	Privacy Office	ICEPrivacy@dhs.gov	(202) 732-3300
ICE	Public Affairs	PublicAffairs.IceOfficeOf@dhs.gov	(202) 732-4242
ICE	Student and Exchange Visitor Program (SEVP) Response Center	SEVIS.Source@DHS.gov	(703) 603-3400
IP	Chemical Facility Anti-Terrorism Standards (CFATS) Help Desk	csat@dhs.gov	(866) 323-2957

IP	Chemical Facility Anti-Terrorism Standards Compliance Assistance Visit Requests	cscd.ieb@hq.dhs.gov	
IP	Chemical Sector Specific Agency	ChemicalSector@dhs.gov	(877) CHEMSEC
IP	CIKR Asset Protection Technical Assistance Program (CAPTAP)	ACAMS-info@hq.dhs.gov	(703) 235-3939
IP	Commercial Facilities Sector-Specific Agency	CFSteam@hq.dhs.gov	
IP	Critical Manufacturing Sector-Specific Agency	cm-ssa@dhs.gov	
IP	Dams Sector-Specific Agency	dams@dhs.gov	
IP	Emergency Services Sector-Specific Agency	ESSTeam@hq.dhs.gov	
IP	Infrastructure Data Taxonomy (IDT)	IICD@dhs.gov	
IP	Integrated Common Analytical Viewer (iCAV)	iCAV.info@hq.dhs.gov	(703) 235-4949
IP	IP Education and Learning Series	IP_Education@hq.dhs.gov	
IP	National Infrastructure Coordination Center (NICC)		(202) 282-9201
IP	National Infrastructure Protection Plan (NIPP)	NIPP@dhs.gov	(703) 603-5069
IP	Nuclear Sector-Specific Agency	nuclearSSA@hq.dhs.gov	
IP	Office for Bombing Prevention	OBP@dhs.gov	(703) 235-5723
IP	Protected Critical Infrastructure Information (PCII) Program	pcii-info@dhs.gov	(202) 360-3023
IP	Protective Security Advisor (PSA) Field Operations Staff	PSAFieldOperationsStaff@hq.dhs.gov	(703) 235-5724
IP	Sector Specific Agency Executive Management Office	SSAexecsec@dhs.gov	
IP	Vulnerability Assessments Branch	IPassessments@dhs.gov.	
S&T	Commercialization Office	SandT_Commercialization@hq.dhs.gov	(202) 254-6749
S&T	Cyber Security Research and Development Center	csrdc@dhs.gov	
S&T	Office of University Programs	universityprograms@dhs.gov	(202) 254-6934
S&T	Project 25 Compliance Assessment Program (P25 CAP)	P25CAP@dhs.gov	
S&T	SAFECOM Program	SAFECOM@dhs.gov	
S&T	SAFETY Act	SAFETYActHelpDesk@dhs.gov	(866) 788-9318
TSA	Cargo Certified Cargo Screening Program	ccsp@dhs.gov	
TSA	Freight and Rail	freightrailsecurity@dhs.gov	
TSA	General Aviation Secure Hotline		1-866-GA-SECUR (1-866-427-3287)
TSA	Highway and Motor Carrier Division	highwaysecurity@dhs.gov	
TSA	Intermodal Security Training and Exercise Program (I-STEP)	i-step@dhs.gov	(571) 227-5150
TSA	Mass Transit	MassTransitSecurity@dhs.gov	
TSA	Office of Airspace Waivers		(571) 227-2071
TSA	Pipeline Security Division	PipelineSecurity@dhs.gov	

TSA	Port & Intermodal Security Division	Maritime@dhs.gov	(571) 227-3556
TSA	Transportation Security Grant Programs	TSAGrants@tsa.dhs.gov	
TSA	TSA Contact Center		1-866-289-9673
CIS Ombudsman	CIS Ombudsman	cisombudsman@dhs.gov	
USCIS	E-Verify	E-Verify@dhs.gov	(888) 464-4218
USCIS	Office of Public Engagement	Public.Engagement@dhs.gov	

Appendix B – Index

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W