Private Sector Resources Catalog 3.0

July 2011

Homeland Security

Intentionally blank page. Please continue to the next page.

Contents

Letter from Assistant Secretary Douglas A. Smith

August 8, 2011

Dear Private Sector Partner,

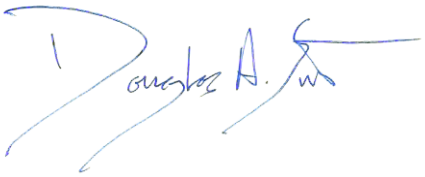
I am pleased to release the Private Sector Resources Catalog 3.0. Developed to facilitate your organization's access to all DHS resources, the Catalog has undergone a second update, and is now reorganized to match the five mission areas of the Quadrennial Homeland Security Review (QHSR): Preventing Terrorism and Enhancing Security, Securing and Managing Our Borders, Enforcing and Administering Our Immigration Laws, Safeguarding and Securing Cyberspace, and Ensuring Resilience to Disasters. This reorganization allows you to quickly find the resources you need. Moreover, all the resources in the Catalog will soon be posted online and fully searchable by any internet search engine. Moving forward, we will update the Private Sector Resources Catalog semi-annually, ensuring that we continue to provide you, our private sector stakeholders, the most up-to-date information and expertise from DHS.

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 coordinates active engagement between DHS and the private sector.

In order to address 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 share the responsibility to build all-hazards preparedness and resiliency into our way of life. As outlined in the QHSR, 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 Office is committed to providing you with the assistance and support you require. You can contact my office 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

Civil Rights and Civil Liberties

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

Community Roundtables CRCL leads, or plays a significant role, in regular roundtable meetings among community leaders and Federal, State, and local government officials. Some of these roundtables bring together American Arab, Muslim, South Asian, Middle Eastern, and Sikh communities with government representatives; other roundtables include immigrant communities and those with frequent DHS contacts. CRCL also conducts roundtables with young leaders of diverse communities. For more information please contact CRCLOutreach@dhs.gov.

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

CRCL Monthly Newsletter is distributed monthly to inform the public about Office activities, including how to make complaints; ongoing and upcoming projects; opportunities to offer comments and feedback; etc. Newsletters are distributed via an email list, posted on the CRCL website (www.dhs.gov/crcl), and made available to community groups for redistribution. Please contact CRCLOutreach@dhs.gov for more information.

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

E-Verify and Unfair Labor Practices Training is provided by CRCL staff on the responsibilities imposed upon the private sector when using E-Verify. Training includes best practices, examples of unlawful practices against workers, and instructions for how to prepare a human resources department. The training assists employer understanding of how to use E-Verify in a responsible manner without violating prohibitions against discrimination. In collaboration with U.S. Citizenship and Immigration Services, CRCL has created two videos, Understanding E-Verify: Employer Responsibilities and Worker Rights and Know Your Rights: Employee Rights and Responsibilities, to ensure employers and employees are knowledgeable about their rights and responsibilities. To view the videos, please visit www.dhs.gov/E-Verify or www.youtube.com/ushomelandsecurity. For more information, contact CRCL at crcltraining@dhs.gov, (202) 357-8258.

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

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

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

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

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

Introduction to Arab American and Muslim American Cultures is an hour-long training DVD, released in the fall of 2006, that provides insights from four national and international experts, including an Assistant United States Attorney who is a practicing Muslim; a member of the National Security Council who is a practicing Muslim; a scholar of Islamic studies; and a civil rights attorney who advocates on issues of concern to Arab American and Muslim American communities. The training assists law enforcement officers and other personnel who interact with Arab and Muslim Americans, as well as individuals from Arab or Muslim communities in the course of their duties. For more information, contact crcl@dhs.gov or visit www.dhs.gov/crcl.

Language Access CRCL provides resources, guidance and technical assistance to recipients of financial assistance from DHS to help ensure meaningful access to persons who are Limited English Proficient (LEP) as required by Title VI of the Civil Rights Act of 1964. CRCL is a member of the Federal Interagency Working Group on LEP, which hosts www.LEP.gov. For more information please contact crcl@dhs.gov.

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

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

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

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

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

DHS Privacy Office sustains privacy protections and the transparency of government operations while supporting the DHS mission. The DHS Privacy Office ensures DHS programs and operations comply with Federal privacy laws and policies. Members of the public can contact the Privacy Office with concerns or complaints regarding their privacy. For more information, visit www.dhs.gov/privacy or contact privacy@dhs.gov, (202) 732-3300.

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

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

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

Victim Assistance Program (VAP) provides information and assistance to victims of Federal crimes, including human trafficking, child exploitation, human rights abuse, and white collar crime. VAP also provides information to victims on post-correctional release or removal of criminal aliens from ICE custody. VAP has developed informational brochures on human trafficking victim assistance, crime victims' rights, white collar crime, and the victim notification program. For further information, please contact VAP at (866) 872-4973.

Health

Commercial Facilities Sector Pandemic Planning Documents are three informational products 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 H1N1 response plan development. The products were created in partnership with International Association of Assembly Manager's Academy for Venue Safety and Security. For

more information, contact the Commercial Facilities SSA at CFSTeam@hq.dhs.gov.

DHS Center of Excellence: Center for Advancing Microbial Risk Assessment (CAMRA) is co-led by Michigan State University and Drexel University and fills critical gaps in risk assessments for decontaminating microbiological threats — such as plague and anthrax — answering the question, "How Clean is Safe?" Resources include: Water mixing and pathogen dilution models; dose response models for Category A bioterror agents; and the Knowledge Warehouse, an online repository of microbial risk assessment information highlighting connections between projects. For more information, visit http://camra.msu.edu or email camra@msu.edu.

DHS Center of Excellence: National Center for Foreign Animal and Zoonotic Disease Defense (FAZD) conducts research to protect 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 Emergency Response Support System; Animal Health Network; 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. For more information, see http://fazd.tamu.edu/ or http://sites.google.com/site/ceezad/home or contact universityprograms@dhs.gov.

DHS Center of Excellence: National Center for Food Protection and Defense (NCFPD) establishes best practices, develops new tools, and attracts 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; Global Chronology of Incidents of Chemical, Biological, Radioactive and Nuclear Attacks from 1961-2005; Mass Production of Detection and Neutralizing Antibodies; Food Protection and Food Safety and Defense Graduate Certificate Programs; 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 Pandemic Influenza Impact on Communications Network Study and Best Practices evaluates the potential impact on the communications infrastructure in the event of a pandemic influenza in the U.S. The study examines potential communications and information technology issues during a pandemic and identifies industry and government recommendations on how to better prepare the nation to handle these challenges. The study is available at http://www.ncs.gov/library/pubs/Pandemic%20Comms%20Impact%20Study%20(December%202007).pdf. For more information, contact ncsweb1@dhs.gov.

Food and Agriculture Sector Criticality Assessment Tool (FASCAT) is a web-based tool used to identify specific systems-based criteria, unique for the Food and Agriculture Sector and utilized for Homeland Infrastructure Threat and Risk Analysis Center data call submissions and identification of infrastructure critical systems for industry owners and operators. For more information, see www.foodshield.org, or contact Food.AG@hq.dhs.gov.

Planning for 2009 H1N1 Influenza: A Preparedness Guide for Small Business DHS, the Centers for Disease Control (CDC), and the Small Business Administration developed this guide to help small businesses understand what impact a new influenza virus, like the 2009 H1N1 flu, might have on their operations, and the importance of a written plan for guiding businesses through a possible pandemic. For more information, see http://www.flu.gov/professional/business/smallbiz.html, or contact IP_Education@hq.dhs.gov.

Sector-Specific Pandemic Influenza Guides are developed for pandemic influenza for the Chemical, Commercial Facilities, Dams, Emergency Services, and Nuclear Sectors. For more information please contact the Sector-Specific Agency Executive Management Office at SSAexecsec@dhs.gov.

Private Sector and Community Engagement

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

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

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

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

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.

Research and Product Development

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

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

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

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

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

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

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

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

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

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

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

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

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

Project 25 Compliance Assessment Program (P25 CAP) was established, in coordination with the National Institute of Standards and Technology (NIST), to provide a process for ensuring that equipment complies with P25 standards, meets performance requirements, and is capable of interoperating across manufacturers. P25 CAP allows emergency responders to confidently purchase and use P25-compliant products. For more information, see http://www.safecomprogram.gov/SAFECOM/currentprojects/project25cap/ or contact P25CAP@dhs.gov.

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

Science & Technology Basic Research Focus Areas represent the technological areas in which S&T seeks to create and/or exploit new scientific breakthroughs and help guide the direction of the S&T research portfolio and to provide long-term science and technology advances for the benefit of homeland security. The focus areas identified by the S&T Research Council, with input from customers and the research community, summarize the fundamental work needed to support the future protection of our Nation. See http://www.dhs.gov/xabout/structure/gc_1242157296000.shtm. Contact the Director of Research, SandT.Research@dhs.gov , and (202) 254-6068.

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

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

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

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

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

Preventing Terrorism and Enhancing Security

Preventing a terrorist attack in the United States remains the cornerstone of homeland security. Our vision is a secure and resilient Nation that effectively prevents terrorism in ways that preserve our freedom and prosperity. Achieving this vision requires us to focus on the core goal of preventing terrorist attacks, highlighting the challenges of preventing attacks using chemical, biological, radiological, and nuclear (CBRN) weapons and managing risks to critical infrastructure.

Bombing Prevention

Bombing Prevention Workshop is a one-day course, intended for regional level public and private stakeholders and planners from emergency management, security, and law enforcement, enhances 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 your State Homeland Security Advisor; see http://www.dhs.gov/xgovt/editorial_0291.shtm for a current list.

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.

Bomb-making Materials Awareness Program (BMAP)/Suspicious Behavior Cards offer simple, concise tips and images helping retailers identify and report suspicious activity and the sale of household items that can be used in making home-made explosives and Improvised Explosive Devices. The register cards give store employees guidance on precursor materials and what to look for regarding suspicious purchases. For more information please contact the Commercial Facilities SSA at CFSTeam@hq.dhs.gov.

Countering IEDs Training for Pipeline Employees is a DVD-based training program to familiarize pipeline company employees and contractors with the threat posed by Improvised Explosive Devices (IEDs). This DVD employs four modules that familiarize viewers with the threat posed by IEDs, how to spot potential IEDs, how to respond to suspicious objects and how to work with responding agencies in the event an IED is discovered or detonated on company property. The DVD incorporates interactive quizzes that can be used by pipeline companies to test employees' knowledge at the end of each module. For more information, contact PipelineSecurity@dhs.gov.

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. For more information, see http://www.northeastern.edu/alert/ and http://energetics.chm.uri.edu. For more information, contact universityprograms@dhs.gov.

Improvised Explosive Device (IED) Awareness / Bomb Threat Management Workshop is a four-hour workshop which enhances and strengthens 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 accommodate up to 50 participants. To request training, contact your State Homeland Security Advisor; see http://www.dhs.gov/xgovt/editorial_0291.shtm for a current list.

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

Improvised Explosive Device (IED) Search Procedures Workshop is an eight-hour workshop consisting of lecture and practical exercises, and 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 your State Homeland Security Advisor; see http://www.dhs.gov/xgovt/editorial_0291.shtm for a current list.

Improvised Explosive Device (IED) Threat Awareness and Detection is the first in a series of web-based trainings, "Threat Awareness & Response for Sporting Events and Public Venues," to be released in three 20-minute modules. The first webinar, IED (improvised explosive device) Threat Awareness and Detection, focuses on identifying IEDs. The training provides awareness-level information for staff, management, and security to recognize, report, and react to unusual activities and threats in a timely manner. For more information, see http://www.dhs.gov/files/programs/gc_1259859901230.shtm or contact CFSTeam@hq.dhs.gov.

Improvised Explosive Device (IED) Threat Awareness and Response is a 20-minute multi-media module on identifying the threat associated with the Improvised Explosive Device (IED). The training is housed on the DHS Homeland Security Information Network (HSIN), and while the target audience is Sports Leagues and Public Venues, much of the material is consistent with general IED Awareness. The module objectives relate to the recognition of IEDs, reporting, and response considerations. For more information, see http://www.dhs.gov/files/programs/gc_1259859901230.shtm or contact CFSTeam@hq.dhs.gov.

Multi-Jurisdiction Improvised Explosive Device (IED) Security Plan (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.

Nuclear Sector Explosive Threat Awareness Training (NSETAT) is provided at no cost to Nuclear Sector stakeholders to educate responders on VBIED threats, use, detection, and mitigation. To increase its accessibility the training will be held regionally across the country. For more information, contact NuclearSSA@hq.dhs.gov.

Training Programs related to the Human Causes and TRIPwire Community Gateway (TWCG) is a 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). Please visit http://www.tripwire.dhs.gov. To request additional information, contact the DHS Office for Bombing Prevention at OBP@dhs.gov.

Chemical Security

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. For more information, see www.dhs.gov/chemicalsecurity or contact (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 Facility Anti-Terrorism Standards (CFATS) Frequently Asked Questions assist 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 are used by the Infrastructure Security Compliance Division (ISCD) in discussions with the chemical industry and those interested in chemical security. If interested in a live presentation about CFATS by ISCD personnel, or to find more information about such presentations see http://www.dhs.gov/files/programs/gc_1224766914427.shtm or contact the CFATS Help Desk at cfats@dhs.gov, (866) 323-2957.

Chemical Facility Anti-Terrorism Standards (CFATS) Risk-Based Performance Standards (RBPS) To assist high-risk chemical facilities subject to CFATS in selecting and implementing appropriate protective measures and practices to meet the DHS-defined RBPSs, ISCD has developed a Risk-Based Performance Standards Guidance document. This document can be found at http://www.dhs.gov/xlibrary/assets/chemsec_cfats_riskbased_performance_standards.pdf. For more information, contact the CFATS Help Desk at cfats@dhs.gov or (866) 323-2957.

Chemical Facility Security: Best Practice Guide for an Active Shooter Incident is a booklet that draws upon best practices and findings from tabletop exercises to present key guidance for chemical facility planning and training, and pose specific questions that an effective active shooter response and recovery plan will answer. To obtain a copy of the guide or for more information, contact ChemicalSector@dhs.gov.

Chemical Security Analysis Center (CSAC) provides a scientific basis for the awareness of chemical threats and the attribution of their use. The CSAC is a resource that provides a centralized compilation of chemical hazard data, using this data in an organized effort for threat analytical purposes. It accomplishes this by providing science and technology-based quality-assured information of the chemical threat to support the unified national effort to secure the Nation; serving as the Nation's source of technical data and information on hazardous chemicals; characterizing the chemical threat through hazard awareness, risk assessments and analyses; advancing knowledge and increase awareness of chemical security hazards to the homeland and to the chemical infrastructure; and utilizing knowledge management techniques to provide definition and direction to identifying and filling data gaps in chemical terrorism related defense posture. For more information, contact george.famini@dhs.gov or 410-417-0901.

Chemical Security Assessment Tool (CSAT) is an online tool developed by the Infrastructure Security Compliance Division (ISCD) to streamline the facility submission and subsequent DHS analysis and interpretation of critical

information used to: preliminarily determine facility risk; assess high-risk facility vulnerability; describe security measures at high risk sites; and, ultimately track compliance with the CFATS program. CSAT is a secure information portal that includes applications and user guides for completing the User Registration, Top-Screen, Security Vulnerability Assessment, and Site Security Plan. For more information, see http://www.dhs.gov/files/programs/gc_1169501486197.shtm or contact the CFATS Help Desk at cfats@dhs.gov, (866) 323-2957.

Chemical Security Compliance Assistance Visit (CAV) Requests are provided by the Infrastructure Security Compliance Division (ISCD) upon request by Chemical Facility Anti-Terrorism Standards (CFATS)-covered facilities. CAVs are designed to provide in-depth knowledge of and assistance to comply with CFATS. For more information, see www.dhs.gov/chemicalsecurity or contact cscd.ieb@hq.dhs.gov.

Chemical Security Summit consists of workshops, presentations, and discussions covering current security regulations, industry best practices, and tools for the Chemical Sector. Designed for industry professionals throughout the Chemical Sector, there is also broad representation from the chemical stakeholder community, including senior DHS officials, congressional staff, and senior government officials. Topics covered at the Summits include: an overview of Chemical Facility Anti Terrorism Standards (CFATS); harmonization of the various chemical regulations; cyber security, State and local issues and freight rail security. Summits also include pre-Summit Demonstrations and post-Summit workshops. For more information, see www.dhs.gov/chemicalsecuritysummit or contact the Chemical SSA at chemicalsector@dhs.gov.

Chemical Sector Classified Briefing The Chemical SSA sponsors a classified briefing for cleared industry representatives twice a year. The intelligence community provides briefings on both physical and cyber threats, as well as other topics of interest for chemical supply chain professionals. For more information please contact the Chemical SSA at chemicalsector@dhs.gov.

Chemical Sector Explosive Threat Awareness Training (CSETAT) Program is a series of one-day training sessions to chemical facility security officers nationwide. The program is designed to increase the Chemical Sector's awareness of the threat of improvised explosive devices (IEDs), including Vehicle Borne IEDs (VBIEDs), provide safety precautions for security professionals dealing with explosive incidents, and enable Chemical Sector professionals to deter, prevent, detect, protect against, and respond to terrorist use of IEDs and VBIEDs. For more information, please contact the Chemical SSA at chemicalsector@dhs.gov.

Chemical Stockpile Emergency Preparedness Program (CSEPP) is a partnership between FEMA and the U.S. Army that provides emergency preparedness assistance and resources to communities surrounding the Army's chemical warfare agent stockpiles. For more information, see http://www.fema.gov/about/divisions/thd_csepp.shtm.

Chemical Sector Industrial Control Systems Security Resource The chemical industry, in partnership with DHS, has collected a wealth of training and reference information designed to assist owners and operators in addressing ICS security. All of this information is compiled on one DVD and is available for free upon request. Please contact ChemicalSector@dhs.gov to request a copy.

Chemical Sector Security Awareness Guide assists owners and operators in their efforts to improve security at their chemical facility and to provide information on the security threat presented by explosive devices and cyber vulnerabilities. To obtain a copy of the guide or for more information, contact ChemicalSector@dhs.gov.

Chemical Sector Training and Resources Database The Chemical Sector-Specific Agency (SSA), within IP's SSA Executive Management Office, works collaboratively with sector partners to develop free, voluntary programs and publications to help mitigate security risk in the sector. To access available resources visit http://www.dhs.gov/files/programs/gc_1276534935062.shtm#content.

Chemical Sector Training Resources Guide contains a list of free or low-cost training, web-based classes, seminars, and documents that are routinely available through one of several component agencies within DHS. The list was compiled to assist facility security officer's train their employees on industry best practices, physical and cybersecurity awareness, and emergency management and response. To obtain a copy of the guide or for more information, contact ChemicalSector@dhs.gov.

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, 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 cfats@dhs.gov, (866) 323-2957.

Infrastructure Protection Sector-Specific Tabletop Exercise Program (IP-SSTEP), Chemical Sector Tabletop Exercise (TTX) is an unclassified and adaptable exercise developed for the purpose of creating an opportunity for public and private critical infrastructure stakeholders and their public safety partners to address gaps, threats, issues, and concerns identified in previous exercises and their after-action processes. The TTX allows participants an opportunity to gain an understanding of issues faced prior to, during, and after a terrorist threat/attack and the coordination with other entities, both private and government, regarding their facility. For more information, contact the Chemical SSA at chemicalsector@dhs.gov.

Monthly Chemical Sector Suspicious Activity Calls The Chemical SSA and Oil and Natural Gas Subsector host a monthly unclassified threat briefing and suspicious activity reporting teleconference for chemical facility owners, operators and supply-chain professionals. To participate, apply for access to HSIN where call-in information is posted to the Chemical Portal. This briefing is scheduled for the fourth Thursday of every month at 11:00AM EDT.

For more information, contact the Chemical SSA at chemicalsector@dhs.gov.

Security Seminar & Exercise Series for Chemical Industry Stakeholders is a collaborative effort between the DHS Chemical SSA and industry stakeholders such as state chemical industry councils, state homeland security offices, industry trade associations and state emergency management agencies. The intent of the program is to foster communication between facilities and their local emergency response teams by encouraging representatives to share their insight, knowledge, and experiences during a facilitated tabletop exercise. The exercise is catered to the specific interests of the organizing entity and can include security scenarios such as an active shooter, a hostage situation, a suspicious package, or a vehicle-borne improvised explosive device. For more information, contact the Chemical Sector-Specific Agency at ChemicalSector@dhs.gov.

Voluntary Chemical Assessment Tool (VCAT) is a secure, web-based application and self-assessment tool designed for use by the chemical industry. The tool allows owners and operators to identify their facility's current risk level using an all-hazards approach. VCAT facilitates a cost-benefit analysis by allowing users to select the best combination of physical security countermeasures and mitigation strategies to reduce overall risk. A webinar demonstrating the tool followed by a Q&A session is available. For more information, contact the Chemical SSA at chemicalsector@dhs.gov.

Web-Based Chemical Security Awareness Training Program is an interactive tool available for 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 participant. For more information, see https://chemicalsecuritytraining.dhs.gov/ or contact the Chemical Sector-Specific Agency at ChemicalSector@dhs.gov.

Who's Who in Chemical Sector Security (October 2008) describes the roles and responsibilities of DHS Components with relation to chemical security. To review the document, please visit http://training.fema.gov/EMIWeb/IS/IS860a/CIKR/assets/ChemicalSectorWhosWho.pdf or for more information, contact the Chemical Sector-Specific Agency at ChemicalSector@dhs.gov.

Committees & Working Groups

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

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

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

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

Dams Security

Active and Passive Vehicle Barriers Guide owners/operators with information on a variety of active and passive vehicle barriers, and properly designing and selecting vehicle barrier systems for Dam Sector operators. For more information, contact dams@dhs.gov.

Analysis Tool is an integrated data management system and dams-specific analysis tool that incorporates a wide range of data input from multiple sources. The tool establishes an integrated analysis gateway for all Dams sector-related tools and information, which allows for a single source for data input and analysis. For more information, contact the Dams SSA at dams@dhs.gov.

Annual Classified Threat Briefing The Dams SSA coordinates this briefing to provide Dams Sector stakeholders with a current threat overview to the U.S., including the Dams Sector and related infrastructure. Dams Sector classified meetings are conducted in person in conjunction with the regularly scheduled Dams Sector meetings. For more information, contact the Dams SSA at dams@dhs.gov.

Comprehensive Facility Reports (CFR) on Dams Sector critical assets**.** These reports support the characterization of critical assets, operational characteristics, and regional interdependency information. By using a standard template across the sector, the CFR takes direct advantage of existing information available from dam safety and inspection reports. For more information, contact the Dams SSA at dams@dhs.gov.

Consequence-Based Top Screen Tool identifies critical facilities within the Dams Sector (e.g., those high-consequence facilities, the failure or disruption of which could be potentially associated with the highest possible impact among sector assets). By focusing on potential consequences and decoupling the analysis from the threat and vulnerability components of the risk process, the CTS approach can serve as an effective all-hazards preliminary prioritization scheme. For more information, contact the Dams SSA at dams@dhs.gov.

Consequence-Based Top Screen Reference Guide on Dams Security includes information pertaining to the methodology, how it was developed, its primary purpose, and the Web-based tool with which it is implemented. For more information, contact the Dams SSA at dams@dhs.gov.

Consequence-Based Top Screen Fact Sheet provides information pertaining to the Consequence-Based Top Screen methodology, including how it was developed, its primary purpose, and the web-based tool with which it is implemented. The fact sheet is available at http://training.fema.gov/EMIWeb/IS/IS860a/CIKR/assets/ConsequenceBased TopScreenMethodologyFactSheet.pdf . For more information, contact dams@dhs.gov.

Crisis Management Handbook provides Dams Sector owners/operators with information relating to emergency response and preparedness issues; includes recommendations for developing emergency action plans and site recovery plans. The handbook is available at http://training.fema.gov/EMIWeb/IS/IS860a/CIKR/assets/DamsSectorCrisisManagementHandbook.pdf . For more information, contact the Dams SSA at dams@dhs.gov.

Dams Sector Councils Fact Sheet provides information pertaining to the partnership framework with which the sector operates, as well as a list of Dams SCC, Dams GCC, and Levee Sub-Sector Coordinating Council members. For more information please contact the Dams SSA at dams@dhs.gov.

Dams Sector Roadmap to Secure Control Systems provides a comprehensive framework and recommendations for the protection of industrial control systems across the Dams Sector in order to enhance sector understanding and management of cyber risks; facilitate the identification of practical risk mitigation solutions; promote information sharing; and improve sector-wide awareness of cybersecurity concerns. For more information, contact the Dams SSA at dams@dhs.gov.

Dams Sector Exercise Series (DSES) is an annual Dams Sector exercise series conducted in collaboration with public and private sector stakeholders in order to identify, analyze, assess, and enhance regional preparedness and disaster resilience, using multi-jurisdictional discussion-based activities involving a wide array of public and private stakeholders. For a given region, this collaborative process is based on a particular scenario that serves as the triggering event to analyze impacts, disruptions, critical interdependencies, and stakeholder roles and responsibilities. The discussion-based process is executed under the framework provided by the Homeland Security Exercise and Evaluation Program. For more information, contact the Dams SSA at dams@dhs.gov.

Homeland Security Information Network – Dams Portal Fact Sheet provides information pertaining to the various components within the Dams Portal, membership structure, and registration process for new members. The fact sheet is available at http://training.fema.gov/EMIWeb/IS/IS860a/CIKR/assets/HSIN-CSDamsPortalFactSheet.pdf. For more information, contact the Dams SSA at dams@dhs.gov.

IS-870 Dams Sector: Crisis Management Overview is a web-based Independent Study training focused on information provided within the Dams Sector Crisis Management handbook. To access this course, see http://training.fema.gov/EMIWeb/ IS/is870.asp . For more information, contact the Dams SSA at dams@dhs.gov.

Illinois Waterway Pilot Project Analysis and Conclusions (FOUO) is a multi-jurisdictional study focused on the development of a regional consequence analysis methodology that captures infrastructure interdependencies and cascading effects associated with lock disruptions and their effects on inland waterway systems. For more information, contact the Dams SSA at dams@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.

IS-871 Dams Sector: Security Awareness (FOUO) is a web-based Independent Study training focused on information provided within the Dams Sector Security Awareness handbook. To access this course: http://training.fema.gov/EMIWeb/IS/is871.asp. For more information, contact the Dams SSA at dams@dhs.gov.

IS-872 Dams Sector: Protective Measures (FOUO) is a web-based Independent Study training focused on information provided within the Dams Sector Protective Measures handbook. To access this course: http://training.fema.gov/EMIWeb/IS/is872.asp. For more information, contact the Dams SSA at dams@dhs.gov.

National Dam Security Forum is conducted in conjunction with the annual Association of State Dam Safety Officials Dam Safety Conference, the forum serves to enhance the security, protection, mitigation, response, recovery, and resiliency capabilities of State dam safety officials, owners/operators, and additional dam stakeholders. Participants are provided with information on a variety of technical and non-technical issues pertaining to the safety, security, and protection of the Nation's dams and related infrastructure. For more information, contact the Dams SSA at dams@dhs.gov.

Overview Brochure provides owners/operators with information regarding the Dams Sector, including the partnership framework with which the sector operators, and the various reference documents developed by the sector. For more information, contact the Dams SSA at dams@dhs.gov.

Personnel Screening Guide for Dams Sector Owners and Operators provides information that assists owners/operators in developing and implementing personnel screening protocols appropriate for their facilities. For more information, contact the Dams SSA at dams@dhs.gov.

Physical Security Measures for Levees Brochure provides information on physical security measures that a levee owner could employee and the factors affecting the selection of those measures. The brochure is available at http://training.fema.gov/EMIWeb/IS/IS860a/CIKR/assets/PhysicalSecurityMeasuresForLeveesBrochure.pdf. For more information please contact the Dams SSA at dams@dhs.gov.

Protective Measures Handbook (FOUO) assists Dams Sector owners/operators in selecting protective measures addressing the physical, cyber, and human elements; includes recommendations for developing site security plans. For more information, contact the Dams SSA at dams@dhs.gov.

Security Awareness Guide is a non-FOUO version of the Dam Sector Security Awareness Handbook to allow for wider distribution to owners/operators. The guide is available at http://www.damsafety.org/media/documents/DownloadableDocuments/DamsSectorSecurityAwarenessGuide_508.pdf. For more information please contact the Dams SSA at dams@dhs.gov.

Security Awareness Guide – Levees assists levee owners in identifying security concerns, coordinating proper response, and establishing effective partnerships with local law enforcement and first responder communities. The guide is available at http://training.fema.gov/EMIWeb/IS/IS860a/CIKR/assets/DamsSectorSecurityAwarenessGuideLevees.pdf?bcsi_scan_24F6D4EFE9292259=0&bcsi_scan_filename=DamsSectorSecurityAwarenessGuideLevees.pdf. For more information, contact the Dams SSA at dams@dhs.gov.

Security Awareness Handbook (FOUO) assists Dams Sector owners/operators in identifying security concerns, coordinating proper response, and establishing effective partnerships with local law enforcement and first responder communities. For more information, contact the Dams SSA at dams@dhs.gov.

Suspicious Activity Reporting Fact Sheet provides information regarding the online Suspicious Activity Reporting tool within the HSIN-CS 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. For more information, contact the Dams SSA at dams@dhs.gov.

Suspicious Activity Reporting Tool is an online reporting tool within the HSIN-CS 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. Accompanied by Fact Sheet/Brochure. For more information, contact the Dams SSA at dams@dhs.gov.

Security Awareness for Levee Owners Brochure provides information on surveillance indicators and incident reporting. The brochure is available at http://training.fema.gov/EMIWeb/IS/IS860a/CIKR/assets/SecurityAwareness ForLeveeOwnersBrochure.pdf. For more information, contact the Dams SSA at dams@dhs.gov.

Research & Development Roadmap: Development of Validated Damage and Vulnerability Assessment Capabilities for Aircraft Impact Scenarios (FOUO) is a collaborative effort involving multiple agencies focused on investigating vulnerabilities of concrete arch and embankment dams to aircraft impact scenarios. For more information, contact the Dams SSA at dams@dhs.gov.

Tabletop Exercise Toolbox (DSTET) (5-11-2011 Under Development) was developed to assist sector stakeholders in planning and conducting a security-based tabletop exercise that is compliant with the Homeland Security Exercise and Evaluation Program. DSTET is a flexible and self-contained product that will provide an effective framework for scenario-driven discussions. This product, which includes a proposed timeline to conduct a four-hour tabletop exercise, is scalable and can be modified to fit specific requirements. Multiple videos and examples are included as part of the tool for use during the exercise as "scene-setters." Toolbox contents include planner instructions, facilitator briefing slides and handbook, situation manual, sample invitation letters, sample feedback forms, and exercise reference materials. For more information, contact the Dams SSA at dams@dhs.gov.

Waterside Barriers Guide provides owners/operators with information on waterside barriers and their use, maintenance, and effectiveness, and elements that must be considered when selecting waterside barriers. For more information, contact the Dams SSA at dams@dhs.gov.

Web-Based Training Fact Sheet provides a brief description and access information for the various web-based training tools developed by the Dams Sector. For more information, contact the Dams SSA at dams@dhs.gov.

General Physical Security Assessment Tools

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 Information (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 Field Operations Branch at FOBanalysts@hq.dhs.gov or 703-235-9349.

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 National Terrorism Alert System threat levels, physical security, personnel security, and information sharing and security. The TSA 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. For more information, see http://www.tsa.gov/assets/pdf/mass_transit_action_items.pdf or contact MassTransitSecurity@dhs.gov.

Critical Manufacturing Partnership Road Show provides Critical Manufacturing Sector members an opportunity to participate in onsite visits to various DHS locations. The visit includes briefings on the current threat to the U.S., including the Critical Manufacturing Sector and related infrastructure. For more information contact CriticalManufacturing@hq.dhs.gov.

Design-Basis Threat (DBT): An Interagency Security Committee Report (FOUO) is a stand-alone threat analysis to be used with the *Physical Security Criteria for Federal Facilities: An ISC Standard*. The DBT document establishes a profile of the type, composition, and capabilities of adversaries. The document is designed to correlate with the countermeasures contained in the compendium of standards and to be easily updated as needed. For more information, see http://www.dhs.gov/files/committees/gc_1194978268031.shtm or contact Isc@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 data in near real time. Data collected during an ECIP visit is consolidated in the IST and then weighted and valued, which enables DHS to develop 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 fobanalysts@hq.dhs.gov (703) 235-9349.

Evacuation Planning Guide for Stadiums This product 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. For more information, contact CFSTeam@hq.dhs.gov.

HS-ANALISER: Homeland Security Analysis, modeLing, Integrated, Secured Environment and Repository for Decision Support is a software system and decision-support tool that allows policy/decision-makers, analysts and researchers to share homeland security risk-focused computing tools, models, data, analysis, and results. For more information, see http://create.usc.edu/research/50831.pdf.

Mass Evacuation Planning Guide for Major Events: NASCAR (FOUO) was developed by DHS and the National Association for Stock Car Auto Racing (NASCAR), and provides a mass evacuation plan template for NASCAR sanctioned facilities. For more information, contact the Commercial Facilities SSA at CFSTeam@hq.dhs.gov.

Protective Measures Guide for U.S. Sports Leagues (FOUO) 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. For more information please contact the Commercial Facilities SSA at CFSTeam@hq.dhs.gov.

Regional Resiliency Assessment Program (RRAP) is a cooperative, DHS-led assessment of specific critical infrastructure and regional analysis of the surrounding infrastructure, including key interdependencies. Private sector critical infrastructure owners and operators interested in receiving more information on the RRAP should contact the Field Operations Branch at resilience@dhs.gov.

Risk Self-Assessment Tool (RSAT) for Stadiums, Arenas and Performing Art Centers is a secure, Web-based application designed to assist managers of stadiums, arenas and performing arts centers 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. For more information please contact the Commercial Facilities SSA at CFSTeam@hq.dhs.gov or RSAT@hq.dhs.gov.

Site Assistance Visits (SAVs) are non-regulatory risk-informed vulnerability assessments that assist critical infrastructure owners and operators in identifying vulnerabilities, protective measures, planning needs, and options for consideration to increase protection from, and

resilience to, a wide range of hazards. Following the assessment, DHS provides owners and operators with an SAV Report, protected as Protected Critical Infrastructure Information (PCII). SAVs enhance critical infrastructure owners' and operators' overall capabilities and resources for identifying and mitigating vulnerabilities, detecting and preventing terrorist attacks, and responding to and recovering from all-hazards events. Private sector critical infrastructure owners and operators interested in receiving more information on SAVs should contact the Field Operations Branch at FOBanalysts@hq.dhs.gov or 703-235-9349.

Hazardous Materials Transportation Security

Federal Motor Carrier Safety Administration: Guide to Developing an Effective Security Plan for the Highway Transportation of Hazardous Materials is a tool that motor carriers transporting hazardous materials can use in developing a security plan as required by the U.S. Department of Transportation in their HM-232 rulemaking [1]. It is designed to provide motor carriers with (a) sufficient background to understand the nature of the threats against hazardous materials transportation; (b) the means to identify the vulnerabilities to those threats; and (c) an approach to address the vulnerabilities. For more information, see http://www.tsa.gov/assets/pdf/guide_security_plan.pdf. Contact the TSA Highway and Motor Carrier offices at highwaysecurity@dhs.gov.

Hazmat Motor Carrier Security Action Item Training (SAIT) Program addresses the TSA recommended security actions that were developed 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 at highwaysecurity@dhs.gov.

Hazmat Trucking Guidance: Highway Security-Sensitive Materials (HSSM) Security Action Items (SAIs) provide security measures for implementation by motor carriers transporting Tier 1HSSM and Tier 2 HSSM. The security practices are voluntary to allow highway motor carriers to adopt measures best suited to their particular circumstances. For more information, see http://www.tsa.gov/what_we_do/tsnm/highway/hssm_sai.shtm or contact highwaysecurity@dhs.gov.

Land Transportation Antiterrorism Training Program

Pipeline and Hazardous Materials Safety Administration: Risk Management Self-Evaluation Framework (RMSEF) provides a basic framework for managing risk as part of the hazardous materials transportation process. RMSEF is a tool for all parties (regulators, shippers, carriers, emergency response personnel, etc.) to look at their operations and consider how they assess and manage risk. For more information, see http://www.phmsa.dot.gov/hazmat/risk/rmsef or contact highwaysecurity@dhs.gov

Hotel, Lodging & Retail Security

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. A variety of resources are available including a Pocket Card, a Brochure, a Booklet, and a Poster. Also, the Pocket Card and Poster are available in Spanish. See the links here: http://www.dhs.gov/xlibrary/assets/active_shooter_pocket_card.pdf, http://training.fema.gov/EMIWeb/IS/IS860a/CIKR/assets/ActiveShooter_Pocket_Printable.pdf, http://www.dhs.gov/xlibrary/assets/active_shooter_booklet.pdf, http://www.dhs.gov/xlibrary/assets/active_shooter_poster.pdf, http://www.dhs.gov/xlibrary/assets/active-shooter-pocket-spanish.pdf, http://www.dhs.gov/xlibrary/assets/active-shooter-poster-spanish.pdf.
For more information contact the Commercial Facilities SSA at CFSteam@dhs.gov.

Active Threat Recognition for Retail Security Officers This 85-minute presentation discusses signs of criminal and terrorist activity; types of surveillance; and suspicious behavioral indicators. 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 email confirmation with instructions for logging in to view the material. For more information, please contact the Commercial Facilities SSA at CFSTeam@hq.dhs.gov.

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.

Hotel and Lodging Advisory Poster was created for all staff throughout the U.S. Lodging Industry 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 is available at http://www.dhs.gov/xlibrary/assets/ip_cikr_hotel_advisory.pdf. For more information, contact the Commercial Facilities SSA at CFSTeam@hq.dhs.gov.

IS-906 Workplace Security Awareness provides guidance to individuals and organizations on how to improve security in the workplace. The Independent Study course is self-paced and takes about an hour to complete. This comprehensive cross-sector training is appropriate for a

broad audience regardless of knowledge and skill level. The course promotes workplace security practices applicable across all 18 critical infrastructure sectors. The training uses innovative multimedia scenarios and modules to illustrate potential security threats. Threat scenarios include: Access & Security Control; Criminal & Suspicious Activities; Workplace Violence; Cyber Threats. The course also features interactive knowledge reviews, employee tools, and additional resources. The training may be accessed on the Federal Emergency Management Agency Emergency Management Institute website: http://training.fema.gov/EMIWeb/IS/IS906.asp. For more information, contact IP_Education@hq.dhs.gov.

IS-907 Active Shooter: What You Can Do provides guidance to individuals, including managers and employees, so that they can prepare to respond to an active shooter situation. The Independent Study course is self-paced and takes about 45 minutes to complete. This comprehensive cross-sector training is appropriate for a broad audience regardless of knowledge and skill level. The training uses interactive scenarios and videos to illustrate how individuals who become involved in an active shooter situation should react. Topics within the course include the actions one should take when confronted with an active shooter and responding law enforcement officials; how to recognize potential indicators of workplace violence; the actions one should take to prevent and prepare for potential active shooter incidents; and how to manage an active shooter incident. This course also features interactive knowledge reviews, a final exam, and additional resources. A certificate is given to participants who complete the entire course. The training may be accessed on the FEMA Emergency Management Institute website: http://training.fema.gov/EMIWeb/IS/IS907.asp. For more information, contact: IP_Education@hq.dhs.gov.

Impact of Post-Event Avoidance Behavior on Commercial Facilities Sector Venues is a literature review conducted to identify studies that quantify direct and indirect economic consequences attributable to avoidance behaviors resulting from terrorist attacks. For more information contact CFSTeam@hq.dhs.gov.

No Reservations: Suspicious Behavior in Hotels is designed to raise the level of awareness for hotel employees by highlighting the indicators of suspicious activity, this video provides information to help employees identify and report suspicious activities and threats in a timely manner. For more information, contact the Commercial Facilities SSA at CFSTeam@hq.dhs.gov.

Protective Measures Guide for the U.S. Lodging Industry (FOUO) provides an overview of best practices and protective measures designed to assist hotel owners and operators in planning and managing security at their facilities. The guide provides examples of successful planning, organizing, coordinating, communicating, operating, and training activities that result in maintaining a safe environment for guests, visitors, and employees. For more information please contact the Commercial Facilities SSA at CFSTeam@hq.dhs.gov.

Retail and Shopping Center Advisory Poster helps train retail employees on the recognition of suspicious behavior that could indicate bomb-making activities; provides specific details on what may be considered suspicious; and encourages reporting suspicious behavior. For more information, contact the Commercial Facilities SSA at CFSTeam@hq.dhs.gov.

Safeguarding Hotels from the Threat of Terrorism was developed in collaboration with the American Hotel & Lodging Association (AHLA), this webinar provides vital, up-to-date information on key terrorism topics with specific reference to recent events, as well as a high-level briefing on the current threat climate for the hotel industry; and specific, protective measures focusing on observing and reporting suspicious activity and items. The webinar focuses on terrorism topics including lessons learned from Mumbai-style attacks; improvised explosive device (IED) awareness and response; and active shooter scenarios. The webinar can be viewed at https://connect.hsin.gov/p23934518/. For more information, contact the Commercial Facilities SSA at CFSTeam@hq.dhs.gov.

Soft Target Awareness Course enhances individual and organizational awareness of terrorism and helps facilitate information sharing at commercial facilities considered soft targets, such as shopping malls and hotels. Facility managers can gain a better understanding of their roles in deterring, detecting, and defending their facilities from terrorism. Each session can accommodate 35 participants or can be modified for one general session for up to 175 participants. To request training, contact your State Homeland Security Advisor; see http://www.dhs.gov/xgovt/editorial_0291.shtm for a current list.

Threat Detection & Reaction for Retail & Shopping Center Staff 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. The presentation can be viewed on the HSIN-CS Commercial Facilities portal at https://connect.hsin.gov/p21849699/. For more information, contact the Commercial Facilities SSA at CFSTeam@hq.dhs.gov.

What's in Store - Ordinary People/Extraordinary Events is a multimedia training video for retail employees of commercial shopping venues to alert them of the signs of suspicious behavior in the workplace that might lead to a catastrophic act. The video is intended to both highlight suspicious behavior, as well as encourage staff to take action when suspicious behavior is identified. The video can be viewed at http://www.dhs.gov/multimedia/dhs_retail_video.wmv. For more information please contact the Commercial Facilities SSA at CFSTeam@hq.dhs.gov.

Infrastructure Protection Education

Critical Infrastructure and Key Resource (CIKR) Asset Protection Technical Assistance Program (CAPTAP) is a weeklong course designed to assist State and local law enforcement, first responders, emergency management, and other homeland security officials understand the steps necessary to develop and implement a comprehensive CIKR protection program in their respective jurisdiction.

The course includes the 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) tools. For more information, see www.dhs.gov/files/programs/gc_1195679577314.shtm or contact TrainingHelp@hq.dhs.gov.

Critical Infrastructure and Key Resources (CIKR) Learning Series features one-hour infrastructure protection web-based seminars on current topics and issues of interest to CIKR owners and operators and key government partners. For more information, see http://www.dhs.gov/files/programs/gc_1231165582452.shtm or contact IP_Education@hq.dhs.gov.

Critical Infrastructure and Key Resources (CIKR) Resource Center was designed to build awareness and understanding of the scope and efforts of each sector 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. For more information, see http://training.fema.gov/emiweb/is/IS860a/CIKR/index.htm or contact IP_Education@hq.dhs.gov (703) 563-3430.

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 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.

Critical Manufacturing Sector-Specific Agency /Transportation Security Administration (TSA) Joint Exercise Programs Working with TSA, this multi-year program provides Critical Manufacturers with planning and execution support from the TSA Intermodal Security Training and Exercise Program (ISTEP) to develop table-top exercises that identify gaps and vulnerabilities in the transportation supply chains of critical manufacturers, within the U.S. and cross-border. For more information, contact criticalmanufacturing@dhs.gov.

Check It!: How to Check A Bag 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 www.dhs.gov/cfsector or by contacting the Commercial Facilities Sector-Specific Agency at CFSTeam@hq.dhs.gov.

Education, Outreach, and Awareness Snapshot is a two-page snapshot describes the National Infrastructure Protection Plan approach to building national awareness and enabling education, training, and exercise programs. The snapshot provides the coordinated approach for establishing national priorities, goals, and requirements for critical infrastructure and key resources (CIKR) protection and resilience. For more information, see http://www.dhs.gov/xlibrary/assets/nipp_education.pdf. or contact NIPP@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 that integrates with the National Infrastructure Protection Plan (NIPP) and accomplish the desired local benefits. This document is available by contacting the NIPP Program Management Office at NIPP@dhs.gov.

IS-821 Critical Infrastructure and Key Resources (CIKR) Support Annex is an Independent Study course that 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.

Infrastructure Protection Sector-Specific Table Top Exercise Program (SSTEP) for the Retail/Lodging and Sports Leagues/Outdoor Venues Subsectors This tool is an unclassified, adaptable and immediately deployable exercise which focuses on information sharing which can be utilized by retail/lodging and outdoor venues/sports leagues organizations at their facilities. In addition to the exercise scenario and slide presentation, users will find adaptable invitational communication tools as well as the after actions report template and participant surveys which will assist in incorporating change and developing improvement plans accordingly. The Retail/Lodging and Sports Leagues/Outdoor Venues SSTEPs will allow participants the opportunity to gain an understanding of issues faced prior to, during, and after a terrorist threat/attack and the coordination with other entities, both private and government, regarding a specific facility. For more information, contact the Commercial Facilities SSA at CFSTeam@hq.dhs.gov.

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

Pipeline Security Awareness for the Pipeline Industry Employee Training CD and Brochures are a security awareness trainings centered on heightening pipeline employee awareness of suspicious activity and their importance in keeping our Nation's pipeline system secure. 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 website at http://www.tsa.gov/what_we_do/tsnm/pipelines/training.shtm. For more information contact the Pipeline Security Division at PipelineSecurity@dhs.gov.

Private Sector Counterterrorism Awareness Workshop This one-day workshop improves 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 training materials enhance and reinforce participants' knowledge, skills, and abilities related to preventing, protecting against, responding to, and recovering from terrorist threats and incidents. This Workshop can accommodate 100 to 250 participants. To request training, contact your State Homeland Security Advisor; see http://www.dhs.gov/xgovt/editorial_0291.shtm for a current list.

Protective Measures Course This two-day course enhances Commercial Facilities 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 Course includes lessons learned and industry best practices in mitigating terrorist attacks. This course can accommodate 35 participants. To request training, contact your State Homeland Security Advisor; see http://www.dhs.gov/xgovt/editorial_0291.shtm for a current list.

Sector-Specific Agency Executive Management Office (SSA EMO) Sector Snapshots, Fact Sheets and Brochures 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. These products include fact sheets and brochures for chemical, commercial facilities, critical manufacturing, dams, emergency services and nuclear sectors. Additional materials are available on request. For more information, contact NIPP@dhs.gov.

SSA EMO/TSA Joint Exercise Program allows Critical Manufacturers to develop advanced tabletop exercises that determine gaps and mitigate vulnerabilities in their respective U.S. and cross-border transportation supply chains. This is a combined program with the Transportation Security Administration (TSA) with support from TSA's Intermodal Security Training and Exercise Program (ISTEP). For more information contact CriticalManufacturing@hq.dhs.gov.

Surveillance Detection Awareness on the Job is a 90-minute interactive web presentation designed to raise awareness of suspicious behaviors that might indicate potential surveillance activities. This virtual production offers cross-sector examples of suspicious activities and behaviors and provides information to help identify and report such behaviors in a timely manner. The webinar features a moderated roundtable discussion of five diverse examples of surveillance and detection. The webinar also provides information about the resources available for timely reporting of suspicious activities and behaviors. The live webinar is available for download on Homeland Security Information Network-Critical Sectors (HSIN-CS). For more information, contact SDAWARE@hq.dhs.gov.

Surveillance Detection Training for Critical Infrastructure and Key Resource Operators and Security Staff explains how protective measures can be applied to detect and deter potential threats to critical infrastructure, as well as the fundamentals for detecting surveillance activity. The three-day course is designed for commercial infrastructure operators and security staff of nationally significant critical infrastructure facilities and can accommodate 25 participants. To request training, contact your State Homeland Security Advisor; see http://www.dhs.gov/xgovt/editorial_0291.shtm for a current list.

Land Transportation

DHS Center of Excellence: National Transportation Security Center of Excellence (NTSCOE) is comprised of seven institutions: University of Connecticut, Tougaloo College, Texas Southern University, Rutgers - The State University of New Jersey, Long Island University, University of Arkansas, and San José State University. The NTSCOE addresses all aspects of transportation security including identification of existing and emerging threats, development of new technologies for resilient infrastructure, establishment of national transportation security policies, training of transportation professionals, and development of undergraduate and graduate education to build and maintain a quality transportation security workforce of the future. For more information, see http://www.ntscoe.uconn.edu/ or contact universityprograms@dhs.gov.

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 ™ website has online training modules for trucking, school buses, law enforcement, cargo, hazmat, highway workers, among others. You can log on to the website for training at: http://www.firstobserver.com/training/home.php or contact or Firstobserver@hms-world.com (888) 217-5902.

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. For more information, see http://www.tsa.gov/what_we_do/tsnm/highway/documents_reports.shtm or contact highwaysecurity@dhs.gov.

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. For more information, contact www.firstobserver.com.

Homeland Security Information Network (HSIN) - Highway and Motor Carrier Portal is part of the Critical Sector section of the HSIN system (HSIN-CS). Membership to the portal is provided once vetted by portal

administrators. For more information, contact HSIN.helpdesk@dhs.gov (866) 430-0162.

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. For more information, see http://www.tsa.gov/what_we_do/layers/istep/index.shtm or contact i-step@dhs.gov (571) 227-5150.

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. For more information, see http://www.tsa.gov/what_we_do/tsnm/highway/documents_reports.shtm or contact highwaysecurity@dhs.gov.

Land Transportation Antiterrorism Training Program (LTATP) is a joint effort by TSA and the Federal Law Enforcement Training Center 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 five-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. For more information, see http://www.fletc.gov/training/programs/counterterrorism-division/land-transportation-antiterrorism-training-program-ltatp or contact: 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. For more information, see http://www.tsa.gov/what_we_do/tsnm/highway/motorcoach.shtm or contact highwaysecurity@dhs.gov.

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 at www.tsa.gov/highway. For more information, contact highwaysecurity@dhs.gov.

School Transportation Security Awareness (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. 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 security awareness information and training to the school transportation industry. For more information, see http://www.tsa.gov/what_we_do/tsnm/highway/stsa.shtm, contact highwaysecurity@dhs.gov.

Transit Agency Security and Emergency Management Protective Measures is a compilation of recommended protective measures for threat levels under the National Terrorism Alert System. 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 NTAS threat conditions and emergencies that might affect a transit agency. For more information, see http://www.tsa.gov/assets/pdf/mass_transit_protective_measures.pdf or contact MassTransitSecurity@dhs.gov.

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. For more information, see www.tsa.gov/grants or contact TSAGrants@tsa.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 website http://www.tsa.gov/what_we_do/tsnm/highway/documents_reports.shtm.

TSA Counterterrorism Guides are designed 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.

Maritime Security

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, see

http://americaswaterwaywatch.uscg.mi or contact aww@uscg.mil 877-24WATCH (877-249-2824).

Area Maritime Security Committees (AMSCs) were established under Title 33 CFR Part 103, July 2003, for the following purposes: 1) identify critical port infrastructure and operations; 2) identify risks, threats, vulnerabilities and consequences; 3) develop and implement strategies to mitigate risks; 4) develop and implement a process for continuously evaluating port security; and, 5) advise and assist the USCG Captain of the Port (in the role of Federal Maritime Security Coordinator) in developing, reviewing and updating the local Area Maritime Security Plan. For more information, see www.homeport.uscg.mil.

DHS Center of Excellence: Coastal Hazards Center of Excellence (CHC) performs research and develops education programs to enhance the Nation's ability to safeguard populations, properties, and economies from catastrophic natural disasters. Resources include Coupled Wave/Storm Surge Prediction Model, Storm Surge Forecasting Tool, In-Situ Scour Evaluation Probe, MUNICIPAL Critical Infrastructure Decision Support Tool, Multi-Modal Mass Evacuation Model, and Youth Coping Response Inventory Tool. For more information, see http://hazardscenter.unc.edu/diem/ and http://www.jsucoe.org/ or contact universityprograms@dhs.gov.

DHS Center of Excellence: Center for Maritime, Island, & Remote/Extreme Environment Security (MIREES) is 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. The MIREES strengthens maritime domain awareness and safeguards populations and properties unique to U.S. islands, ports, and remote and extreme environments. For more information, see http://cimes.hawaii.edu/ and http://www.stevens.edu/csr/ or contact universityprograms@dhs.gov.

Harbor Safety Committees are a cooperative means to inform mariners about vessel traffic hazards and to reduce the risk of navigation incidents. They may be established by local agreements, chartered by States, or organized by the Coast Guard. Harbor Safety Committees advise their respective Captains of the Ports. Some States require their Harbor Safety Committees to deliver safety plans and identify safety concerns to their respective lead State agencies. Members of Harbor Safety Committees typically include representatives from the shipping industry, fishing industry, tug operators, vessel pilots, marine patrols, and government, public or private environmental organizations. For more information, see the AMSC, Area Committee and HSC postings at www.homeport.uscg.mil.

HOMEPORT is the primary on-line means of communicating alerts, announcements and other information from the Coast Guard field units to their partners, including the private sector. Homeport also provides public and protected community-of-interest chat and interactive information between partners. Specific Homeport Topics Include: containers, domestic vessels (U.S. flag vessels), environmental, facilities, incident management and preparedness, investigations (maritime casualties and incidents), marine safety, maritime domain awareness and information sharing, maritime security, and waterways, regulations/administrative adjudications, vessel standards, counter-piracy, Maritime Transportation Security Act (MTSA), Marine Safety Center, Mariner Credential Verification, and Mariner Credential Application Status. For more information, see http://homeport.uscg.mil.

Maritime Passenger Security Courses address topics to improve passenger vessel employee 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 for Passenger Vessels and Terminals," and "Crowd Control for Passenger Vessels and Terminals," and "Maritime Terrorism and Hijacking Situations." To order, contact TSA Port & Intermodal Security Division at Maritime@dhs.gov (571) 227-3556.

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

The Coast Guard Journal of Safety at Sea is the voice of the Coast Guard Marine Safety and Security Council and is published quarterly with over 30,000 copies mailed out for each issue. Each edition of Proceedings is typically 80 to 100 pages and features a specific theme and assigned based on the command's expertise in that area. The audience includes a large segment of the private maritime industry population, including retired officers, fishing vessel captains, river pilots, ocean scientists, marine engineers, tug/tow boat operators, shipping executives, insurance operators, and maritime lawyers. Issues of Proceedings are available to the public at www.uscg.mil/proceedings.

Port Interagency Information Sharing Assessment consists of a recurring process of interviews with Coast Guard Sector personnel and selected Federal, State, local personnel, and private partners who participate in joint maritime planning, prevention, response and recovery missions. The field interviews are conducted by a team from the Coast Guard Headquarters Information Sharing Executive Agent staff, who transcribe best practices and recommended improvements, and produce an annual report of findings for internal improvement. Port Interagency Information Sharing reports are currently only released to the participants, although a publicly-releasable version of the report is under consideration for 2012. To schedule participation in next year's annual interviews, please contact the study team at uscginformationsharing@uscg.mil.

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. For more information, visit http://www.fema.gov/government/grant/ or contact askcsid@dhs.gov (800) 368-6498.

Secure Freight Initiative (SFI) and Importer Security Filing and additional carrier requirements (10+2) The Secure Freight Initiative, through partnerships with foreign governments, terminal operators, and carriers, enhances the DHS capability to 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 U.S. 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 contact securefreightinitiative@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. For more information, see http://www.tsa.gov/what_we_do/layers/twic/index.shtm, or contact (866) 347-8942.

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, assists the Coast Guard with homeland security duties, teaches boating safety classes, conducts free vessel safety checks for the public, and performs many other support 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 National Maritime Center (NMC) issues Merchant Mariner Credentials (MMC) to fully qualified U.S. mariners, approves and audits training programs and courses offered by mariner training organizations throughout the U.S., 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).

U.S. Coast Guard Navigation Center supports safe and efficient maritime transportation by delivering accurate and timely maritime information, vessel monitoring system support and Global Position System (GPS) augmentation signals that permit high-precision positioning and navigation. The Navigation Center accomplishes its missions through the operation of the Differential GPS (DGPS) Control Station, Long Range Identification and Tracking (LRIT) Business Help Desk, Nationwide Automated Identification System (NAIS) System Operations Center (SOC), the Navigation Information Service (NIS) and serves as the Deputy Chair to the Civil GPS Service Interface Committee (CGSIC). For additional information, see http://www.navcen.uscg.gov/.

Vessel Documentation (for US Flag Vessels) The National Vessel Documentation Center facilitates maritime commerce and the availability of financing while protecting economic privileges of U.S. 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).

Mass Transit and Rail Security

Freight Rail Security Grant Program funds freight railroad carriers, 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 askcsid@dhs.gov (800) 368-6498.

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. For more information, contact HSIN.helpdesk@dhs.gov or Linda.Lentini@dhs.gov (866) 430-0162.

Homeland Security Information Network – Public Transit Portal (HSIN-PT) has been integrated into the HSIN 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. Finally, a preplanned alert notification system enables communication 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. For more information, contact MassTransitSecurity@dhs.gov.

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 askcsid@dhs.gov (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 askcsid@dhs.gov (800) 368-6498.

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.

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 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. For more information, contact MassTransitSecurity@dhs.gov.

Mass Transit and Passenger Rail - Field Operational Risk and Criticality Evaluation (FORCE) is a threat-based, risk-managed protocol that 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 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 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 Security and Safety Roundtables TSA, the Federal Transit Administration (FTA), and FEMA co-sponsor the annual Transit Security and Safety Roundtables, bringing together law enforcement chiefs; security directors and safety directors from the Nation's 60 largest mass transit and passenger rail agencies; Amtrak; and Federal security partners to discuss terrorism prevention and response challenges and to work collaboratively in developing 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 Training Program Guidelines is 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, FEMA, and TSA; that are available to ensure employees are trained in the designated areas. For more information, see http://www.tsa.gov/assets/pdf/TSGP_Training_IB243.pdf, for TSGP – Approved Training Programs, see http://www.tsa.gov/assets/pdf/approved_vendor_list.pdf or MassTransitSecurity@dhs.gov.

Mass Transit Smart Security Practices is 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. This compilation fosters communication nationally among security professionals in mass transit and passenger rail to expand adoption of effective practices, tailored as necessary to each agency operating environment. For more information, contact MassTransitSecurity@dhs.gov.

Motorcoach Guidance: Security and Emergency Preparedness Plan (SEPP) is a guideline and template that you may use in developing a SEPP. The steps involved in this process include an evaluation of current security procedures, an identification of threats and vulnerabilities to your operation, and the development of policies and procedures to effectively address deficiencies. For more information see, http://www.tsa.gov/assets/doc/sepp.doc or contact highwaysecurity@dhs.gov.

Rail Security Rule Overview On November 26, 2008, DHS 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. For more information, see http://www.tsa.gov/assets/pdf/rail_rule_overview_for_stakeholder_workshops_mar_09.pdf or contact Scott.Gorton@dhs.gov.

News Sources

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

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

CBP Newsroom, News Magazine and Alerts compiles the latest information on noteworthy occurrences documenting apprehensions of criminals, seizures of illegal drugs, rescues missions, and many other agency success stories from around the country. These highlights can be found at http://www.cbp.gov/xp/cgov/newsroom/ CBP also publishes a news magazine: http://www.cbp.gov/xp/cgov/newsroom/publications/frontline_magazine/ and advisories/alerts for travelers and the trade community: http://www.cbp.gov/xp/cgov/newsroom/advisories/.

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.

Daily Open Source Infrastructure Report is collected each weekday 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). For more information, see http://www.dhs.gov/files/programs/editorial_0542.shtm or contact NICCReports@dhs.gov or CIKR.ISE@dhs.gov (202) 312-3421.

FEMA Private Sector E-alerts are periodic e-alerts providing timely information on topics of interest to private sector entities. The FEMA Private Sector Web Portal aggregates FEMA 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.

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

Nuclear Security

Nuclear Sector Overview introduces readers to the Nuclear Reactors, Materials, and Waste Sector. It includes facts, roles and responsibilities, and sector initiatives and activities. For more information, contact NuclearSSA@hq.dhs.gov.

Nuclear Sector Voluntary Security Programs Fact Sheet provides a listing of select voluntary protection and resilience products and initiatives in the sector. For more information, contact NuclearSSA@hq.dhs.gov.

Tracking of Radioactive Sources Focus Group White Paper: Deliverable of the Tracking of Radioactive Sources Focus Group of the Radioisotopes Subcouncil of the Nuclear Sector and Government Coordinating Council The Tracking of Radioactive Sources Focus Group was created as a public-private working group of the NSCC-NGCC to identify and evaluate existing commercially available passive and active tracking technologies and their applicability for the tracking of conveyances, packages, and/or individual radioactive sources. Improved tracking capabilities could enhance the security of risk-significant quantities of radioactive material during transport. The identified White Paper constitutes the final deliverable of the Tracking of Radioactive Sources Focus Group. For more information, contact the Nuclear SSA at NuclearSSA@hq.dhs.gov.

Who's Who in DHS Nuclear Sector Infrastructure Protection describes the roles and responsibilities of the DHS components with relation to the nuclear sector. For more information, contact NuclearSSA@hq.dhs.gov.

Passenger and Cargo Aviation Security

Air Cargo Screening Technology List-For Passenger Aircraft lists the Non-Sensitive Security Information version of the Transportation Security Administration Air Cargo Screening Technology List-For Passenger Aircraft. The document lists the equipment that can be used by air carriers, indirect air carriers, independent cargo screening facilities, and shippers in the Certified Cargo Screening Program to screen for domestic and outbound (of the United States) air cargo. This information contains Qualified, Approved, and Waived technologies, their manufacturer, model number, and top assembly part number. This information can be found at http://www.tsa.gov/assets/pdf/non_ssi_acstl.pdf.

AIRBUST Program provides the general public and aviation community with a forum to share information on suspicious small aircraft. An AIRBUST poster and pocket-sized laminated card display the phone number for reporting suspicious activity or low-flying aircraft, 1-866-AIRBUST (1-866-247-2878). This number rings directly to the CBP Air and Marine Operations Center (AMOC) operations floor. The two-sided laminated card displays drawings of single-and twin-engine aircraft often used to transport contraband and lists helpful information to include when calling. The AIRBUST poster 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.

Aviation Safety & Security Program provides hands-on education and covers the use of models and tools for evaluation of security and anti-terrorism within a modular format. The short courses also provide training in the methods of analysis. Short courses designed for police and fire departments help personnel develop safety programs that can be used in the event of terrorism. For more information, see http://www.viterbi.usc.edu/aviation/.

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 to detect, deter, and report potential or actual security threats. Air Cargo Watch materials include 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. For more information, see http://www.tsa.gov/what_we_do/layers/aircargo/watch.shtm.

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/.

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 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.

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/training.shtm.

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).

Certified Cargo Screening Program provides a mechanism by which industry may achieve 100% screening of cargo on passenger aircraft without impeding the flow of commerce. Informational materials include: one-page overview of CCSP, CCSF and Chain of Custody Standards, a tri-fold brochure, supplemental CCSP program material with at a glance program overview of the program, a quick hits overview with impact of 100% screening, and supplemental CCSP materials. For more information, see www.tsa.gov/ccsp or contact ccsp@dhs.gov or the TSA Contact Center, (866) 289-9673.

DCA Access Standard Security Program (DASSP) TSA's Interim Final Rule, which was developed in coordination with other DHS Agencies and the Department of Defense, takes into consideration the special security needs of Washington Reagan National Airport (DCA). Under the TSA 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). For more information, 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 and the Washington, D.C. Flight Restricted Zone. For more information, see http://www.tsa.gov/what_we_do/tsnm/general_aviation/programs_sp.shtm#maryland or contact (571) 227-2071.

General Aviation Security Guidelines are for security enhancements at the Nation's privately and publicly owned and operated general aviation (GA) landing facilities. The 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.

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.

Paperless Boarding Pass Pilot enables passengers to download their boarding pass on their cell phones or personal digital assistants. This 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.

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. For more information, please visit http://www.cbp.gov/xp/cgov/travel/. For additional questions or concerns, please contact CBP via e-mail at Private.Aircraft.Support@dhs.gov.

Recommended General Aviation Security Action Items for General Aviation Aircraft Operators and Recommended Security Action Items for Fixed Base Operators are 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.

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. For more information, see http://www.tsa.gov/assets/pdf/sfbop_general_faq.pdf or contact tsnmfbo@dhs.gov.

Secure Flight enhances the security of domestic and international commercial air travel, while also enhancing the travel experience for passengers, through the use of improved, uniform watchlist matching performed by TSA agents. Secure Flight also incorporates an expedited and integrated redress process for travelers who think they have been misidentified or have experienced difficulties in their air travel. Resources available for aviation stakeholders include a communications toolkit, brochure, privacy information, signage, and an 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.

User's Guide on Security Seals for Domestic Cargo provides information on the 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.

Protecting Against Fraud & Counterfeiting

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

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

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

eInformation Network The Secret Service eInformation Network is available – for free – to authorized law enforcement officers, financial institution investigators, academic partners, and commercial partners of the Secret Service. The site contains three tools: the eLibrary, a unique collection of resource databases which allows authorized users from throughout the law enforcement community to obtain information on a range of sensitive topics including counterfeit corporate checks, credit card issuing bank information, and recovered skimming devices; an Electronic Crimes Task Force component that serves as an efficient, secure web-based collection of best practices, vulnerability guides, National Infrastructure Protection Center (NIPC) advisories, and a subject-specific issue library; and the US Dollars Counterfeit Note Search, a site that provides the user with the ability to conduct a search of the Secret Service counterfeit note database. For more information, see www.einformation.usss.gov.

Electronic Crimes Task Force (ECTF) Program brings together not only Federal, State and local law enforcement, but also prosecutors, private industry and academia. The common purpose is the prevention, detection, mitigation and aggressive investigation of attacks on the nation's financial and critical infrastructures. The U.S. Secret Service's ECTF and Electronic Crimes Working Group initiatives prioritize investigative cases that involve electronic crimes. These initiatives provide necessary support and resources to field investigations that meet any one of the following criteria: significant economic or community impact, participation

of organized criminal groups involving multiple districts or transnational organizations, or the use of schemes involving new technology. For more information, see http://www.secretservice.gov/ectf.shtml.

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

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

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

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

Intellectual Property Rights (IPR) Enforcement: A Priority Trade Issue The trade in counterfeit and pirated goods threatens America's innovation economy, the competitiveness of our businesses, the livelihoods of U.S. workers, national security, and the health and safety of consumers. The trade in these illegitimate goods is associated with smuggling and other criminal activities, and often funds criminal enterprises. For more information, visit 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. The CBP on-line recordation allows intellectual property owners to electronically record their trademarks and copyrights with CBP, and makes IPR recordation information readily available to CBP personnel, facilitating IPR seizures by CBP. CBP uses recordation information to actively monitor shipments and prevent the importation or exportation of infringing goods. For more information, see http://iprs.cbp.gov/ or contact hqiprbranch@dhs.gov (202) 325-0020.

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

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

Intellectual Property Rights (IPR) U.S. – EU Joint Brochure and Web Toolkit for Trademark, Copyright Owners 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 Agencies 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, visit http://www.cbp.gov/linkhandler/cgov/trade/priority_trade/ipr/pubs/cpg_final_090306.ctt/cpg_final_090306.pdf. To access the Toolkit, visit http://www.cbp.gov/linkhandler/cgov/trade/priority_trade/ipr/pubs/cpg_final_090306.ctt/cpg_final_090306.pdf or contact the IPR Help Desk at ipr.helpdesk@dhs.gov or (562) 980-3119 ext. 252.

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

Operation In Our Sites specifically targets websites and their operators that distribute counterfeit and pirated items over the Internet, including counterfeit pharmaceuticals and pirated movies, television shows, music, software, electronics, and other merchandise, as

well as products that threaten public health and safety. For more information, visit http://www.ice.gov/doclib/news/library/factsheets/pdf/operation-in-our-sites.pdf.

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

Operation Guardian is a multi-agency effort to combat the increasing importation of substandard, tainted, and counterfeit products that pose a health and safety risk to consumers. The identification of these commodities has led to the successful detention and seizure of numerous containers of hazardous products. For more information, visit http://www.ice.gov/news/library/factsheets/guardian.htm

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

Protecting, *Analyzing*, & Sharing Information

Automated Critical Asset Management System (ACAMS) is a secure, web-based portal developed in partnership with State and local communities and the State, Local, Tribal, Territorial Government Coordinating Council (SLTTGCC). ACAMS is designed to help State and local governments build critical infrastructure protection programs in their local jurisdictions and implement the National Infrastructure Protection Plan (NIPP). ACAMS provides a set of tools and resources that help law enforcement, public safety and emergency response personnel inventory, analyze and utilize critical infrastructure information to prepare, prevent, respond to and recover from an attack, natural disaster, or emergency. ACAMS is provided at no cost for State and local use and is protected from public disclosure through the Protected Critical Infrastructure Information (PCII) program. For more information, see www.dhs.gov/ACAMS or contact ACAMShelp@hq.dhs.gov (866) 634-1958.

Automated Critical Asset Management System (ACAMS) Web-Based Training provides Federal, State, local first responders, emergency managers, and Homeland Security officials with training on the use and functionality of the ACAMS tool. Completion of training is required in order to access information within ACAMS. For more information, contact Traininghelp@hq.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 Open Source Enterprise Daily and Weekly 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 Human Trafficking and Smuggling Report, The DHS Daily Terrorism Report, and The DHS Weekly Weapons and Munitions 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".

Homeland Security Information Network (HSIN) is a web-based knowledge management tool designed to increase collaboration between Federal, State, local, Tribal, territorial, private sector, and international entities. It provides a reliable and secure system for information sharing between partners engaged in the homeland security mission. HSIN is composed of many diverse compartments called *Communities of Interest* (COI). Each COI is designed and maintained by its own administrators. HSIN is a secure system and access to compartments is granted by invitation only. A single user may be invited to multiple COIs depending on their need to access that information. Applications can be obtained by sending a request to HSIN.Outreach@hq.dhs.gov. For more information, visit www.dhs.gov/hsin or contact the HSIN Help Desk: 1-866-430-0162; hsin.helpdesk@dhs.gov.

Homeland Security Information Network-Critical Sectors (HSIN-CS) is the primary information-sharing platform between the critical infrastructure 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. Pre-cleared 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.

ICE LINK Portal is a web-based communications and collaboration platform administered by the National Incident Response Unit (NIRU). 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 first responder personnel in the private sector in the event of a national crisis or incident. For more information and/or assistance, contact niru@dhs.gov.

Identity Management enhances security and privacy of information sharing environments by improving authentication for persons, hardware devices, and software applications across all levels of government to enable seamless and secure interactions among Federal, state, local, and private sector stakeholders ensuring that they have comprehensive, real-time, and relevant information. For more information, please contact SandT-Cyber-Liaison@hq.dhs.gov.

Infrastructure Information Collection System (IICS) is a secure, web-based application designed to provide infrastructure owners with the ability to easily access, search, retrieve, visualize, analyze, and export infrastructure data originating from multiple disparate sources through a single interface. The IICS enables access to infrastructure-related data that is owned and managed by IP through the Infrastructure Data Warehouse as well as infrastructure-related data from various other Federal, State, and local infrastructure protection mission partners. By enabling data from multiple sources and contained within multiple databases to be linked and accessed through one location, the IICS eliminates the need for information to be housed and managed within a single database or by a single entity. For more information, contact IICD-IICS@hq.dhs.gov.

Intelligence and Analysis Private Sector Partnership Program 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 pre-cleared 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.

Joint DHS/FBI Classified Threat and Analysis Presentations provide 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 network 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 an approximately quarterly to semi-annual basis, with additional sessions as threat developments may warrant. For more information, contact MassTransitSecurity@dhs.gov.

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.

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. For more information, see http://www.biometrics.gov/nstc/Default.aspx or contact info@biometrics.org.

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, the Final Rule, and the PCII Program Procedures Manual. Information about the PCII Program, including the CII Act of 2002, the Final Rule and the implementing regulation as well as the PCII Program Procedures Manual can be found at www.dhs.gov/pcii. For additional information, contact pcii-info@dhs.gov or (202) 360-3023.

Technical Resource for Incident Prevention (TRIPwire) is the DHS 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 to anticipate, identify, and prevent IED incidents. To request

additional information, contact DHS Office for Bombing Prevention at OBP@dhs.gov or view www.tripwire-dhs.net.

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

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 website comes from the USCG Marine Information for Safety and Law Enforcement (MISLE) information system. For more information, see http://cgmix.uscg.mil/.

Terrorism Prevention

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

DHS Center of Excellence: Global Terrorism Database is an open-source database including information on terrorist events around the world from 1970 through 2008 (with additional updates planned for the future). For more information, see www.start.umd.edu/gtd.

Training Programs related to the Human Causes and Consequences of Terrorism are customized training programs for professional audiences. Training modules explore such topics as global trends in terrorist activity, impact of counterterrorism efforts, terrorist activity in specific regions/countries, terrorist target selection and weapon choice, nature of terrorist organizations, and planning resilient communities. Modules and programs can be delivered in a range of modes, including in-person seminars or mini-courses, or online programs. The cost of a program varies dependant on the level of customization and the mode of delivery. For more information, see http://www.start.umd.edu/start/ or universityprograms@dhs.gov.

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

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. For more information, see www.start.umd.edu.

DHS Geospatial Information Infrastructure (GII) is a body of geospatial data and application services built to meet common requirements across the DHS mission space. OneView (https://gii.dhs.gov/oneview) is a lightweight, web-based geographic visualization and analysis that provides a method for individual users to access and interact with all GII services. The GII also maintains the DHS Earth KML service, which provides authoritative infrastructure data and various static and 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. For more information, contact iCAV.info@hq.dhs.gov.

Expert Judgment and Probability Elicitation consists of methodologies and tools for elicitation of expert judgments and probabilities that are often required in the quantification of risk and decision models related to terrorist threats. This is the case when data is inconclusive or there is controversy about how evidence should be interpreted. For more information, see http://create.usc.edu/research/Expert Judgment Elicitation Methods.pdf or contact universityprograms@dhs.gov.

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

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, DHS 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. For more information, see

http://www.dhs.gov/files/publications/gc_1226595934574.shtm or visit https://taxonomy.iac.anl.gov/ to use this tool or contact: IDT@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 Field Operations Branch at FOBanalysts@hq.dhs.gov or 703-235-9349.

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

National Critical Infrastructure and Key Resources (CIKR) Protection Annual Report Snapshot is a two-page snapshot describing the National CIKR Protection Annual Report that is developed from the Sector Annual Reports. The Annual Reports are a presidentially-required report to the Secretary of Homeland Security on efforts to identify, prioritize, and coordinate CIKR protection in their respective sectors. For more information, see http://www.dhs.gov/xlibrary/assets/nipp_annrpt.pdf. For more information, contact NIPP@dhs.gov.

National Infrastructure Advisory Council (NIAC) provides advice to the President, through the Secretary of Homeland Security, 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) 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. For more information, see http://www.dhs.gov/files/programs/editorial_0827.shtm or to request materials contact the NIPP Program Management Office NIPP@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.

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.

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 askcsid@dhs.gov (800) 368-6498.

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

Physical Security Criteria for Federal Facilities: An Interagency Security Committee Standard (FOUO) The standard establishes a baseline set of physical security measures to be applied to all Federal facilities based on their designated facility security level. It also provides a framework for the customization of security measures to address unique risks faced at each facility. The interim standard will be used during a 24 month validation period to confirm the need and usability of this standard. For more information, see http://www.dhs.gov/files/committees/gc_1194978268031.shtm or contact the ISC at Isc@dhs.gov.

Pipeline Security Guidelines In December 2010 TSA released Pipeline Security Guidelines that supersede previous Federal documents as the primary guide for pipeline industry security. The revised Pipeline Security Guidelines were developed in cooperation with industry and government members of the Pipeline Sector and Government Coordinating Councils, industry association representatives and other interested parties. The Guidelines are intended to be used by natural gas and hazardous liquid transmission pipeline companies, natural gas distribution companies and liquefied natural gas

facility operators. For more information, see http://www.tsa.gov/what_we_do/tsnm/pipelines/resources.shtm or contact PipelineSecurity@dhs.gov.

Protective Security Advisor provide 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: fobanalysts@hq.dhs.gov or (703) 235-9349.

Science and Technology Directorate Career Development Grants (CDG) Program provides competitive awards to support undergraduate and graduate students attending institutions, including the Centers for Excellence, which have made a commitment to develop Homeland Security-related Science, Technology, Engineering, and Mathematics (HS-STEM) curricula and fields of study. These two competitive programs provide educational support, internships, and employment avenues to highly qualified individuals to enhance the scientific leadership in areas important to DHS. DHS requires supported students to serve one 10-week summer internship and one year in an approved HS-STEM venue. Student and scholar researchers perform work at more than 28 DHS-affiliated venues including the S&T Directorate, national laboratories, and DHS Components such as the United States Coast Guard and the Office of Intelligence and Analysis (I&A). For more information, visit http://www.grants.gov/search/search.do?mode=VIEW&oppId=60714.

Sector Annual Reports (FOUO) Collaborating with government and private sector to develop, update, and maintain Sector Annual Reports for the Chemical, Commercial Facilities, Critical Manufacturing, Dams, Emergency Services, and Nuclear Sectors. For more information please contact the Sector-Specific Agency Executive Management Office at SSAexecsec@dhs.gov.

Sector-Specific Plans (FOUO) 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.

SSA EMO Classified Threat Briefings SSA EMO coordinates both regularly scheduled and incident-specific classified briefings for cleared sector partners. For more information, contact the Sector-Specific Agency Executive Management Office at SSAexecsec@dhs.gov.

Terrorist Organization Profiles is a collection of information on terrorists organizations and is developed and sponsored by the Memorial Institute for the Prevention of Terrorism (MIPT). Through this project, MIPT collects information on terrorist groups and key leaders of terrorist groups. The Terrorist Organization Profiles (TOPs) presents data collected for and by MIPT through March 2008. For more information, see http://www.start.umd.edu/start/data_collections/tops/.

The Evolving Threat: What You Can Do Webinar discusses analysis of the latest intelligence analyzed by the DHS Office of Intelligence and Analysis (I&A), and consists of a brief synopsis of evolving threats, followed by a protective measures presentation. Additionally, the protective measures portion of the webinar is available at https://connect.HSIN.gov/p55204456. For more information, please contact the Commercial Facilities SSA at CFSTeam@hq.dhs.gov.

Securing and Managing Our Borders

A safe and secure homeland requires that we maintain effective control of our air, land, and sea borders. Secure, well-managed borders must not only protect the United States against threats from abroad; they must they must also expedite the safe flow of lawful travel and commerce. We must achieve effective control of the physical borders and approaches to the United States, we must work together to look beyond our borders to identify and disrupt threats before they reach our shores, and we must disrupt and dismantle transnational criminal and terrorist organizations that smuggle or traffic people, illicit goods, or the proceeds of crime across the U.S. border, and commit violent acts.

Border Security

1-800 BE ALERT The public can report 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.

DHS Center of Excellence: National Center for Border Security and Immigration (NCBSI), co-led by the University of Arizona at Tucson and the University of Texas El Paso, conducts research and develops educational activities through the development of technologies, tools and advanced methods to balance immigration and trade with effective border security, as well as assessing threats and vulnerabilities, improving surveillance and screening, analyzing immigration trends, and enhancing policy and law enforcement efforts. For more information, see http://www.borders.arizona.edu/ and http://osi.utep.edu/NCBSI/index.html or contact universityprograms@dhs.gov.

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 provide nationwide first responder and law enforcement contact numbers and electronic linkage to registered participants. Reported caller information is entered into a secure 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.

ICE National Border Enforcement Security Task Force (BEST) Unit (NBU) ICE Homeland Security Investigations (HSI) in partnership with CBP, Federal, international, State, and local law enforcement agencies, expanded its ongoing Border Crimes Initiative by creating a multi-agency initiative called the BEST. The program is designed to identify, disrupt, and dismantle organizations that seek to exploit vulnerabilities along the U.S. borders and threaten the overall safety and security of the American public. The BESTs are designed to increase information sharing and collaboration among the participating agencies, focusing toward the identification, prioritization, and investigation of emerging or existing threats. For more information, see http://www.ice.gov/news/library/factsheets/best.htm.

ICE Tip-Line is a 24/7 toll free number enabling the public to report violations of immigration and customs laws, sexual and economic exploitation of children and adults, threats to national security and other activities considered illegal or suspicious in nature. For more information, see http://www.ice.gov/news/library/factsheets/lesc.htm or by calling (866) DHS-2ICE (1-866-347-2423) or outside the United States: +1 (877) 347-2423.

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, the ICE 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 and U.S. companies that manufacture, sell or export strategic technology and munitions. For more information, see http://www.ice.gov/project-shield/ or contact ICE Headquarters, PSA Program Manager at (202) 732-3765 or (202) 732-3764.

Trade Facilitation

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, 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, visit http://www.cbp.gov/xp/cgov/trade/automated/automated_systems/ams/.

Automated Commercial Environment (ACE) is the U.S. 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, visit http://www.cbp.gov/xp/cgov/trade/automated/modernization/.

Automated Commercial Environment (ACE) National Help Desk provides customer technical support services 24 hours a day, 7 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, call (800) 927-8729.

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, see http://www.cbp.gov/xp/cgov/trade/automated/automated_systems/acs/ or contact (571) 468-5000.

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, see http://www.cbp.gov/xp/cgov/trade/automated/automated_systems/client_reps.xml or (571) 468-5000.

CBP INFO Center Self Service Q&A Database is a searchable database with over 600 answers to 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, 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.

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, visit http://www.cbp.gov/xp/cgov/trade/trade_outreach/.

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. Through this initiative, businesses 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, visit http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/. For questions or concerns, contact the CBP Industry Partnership Program at (202) 344-1180 or industry.partnership@dhs.gov.

Importer Self Assessment – Product Safety Pilot (ISA-PS) CBP and the Consumer Product Safety Commission (CPSC) developed this self-assessment for importers to prevent unsafe imports from entering the U.S. For more information, visit http://www.cbp.gov/xp/cgov/trade/trade_programs/importer_self_assessment/isa_safety_pilot.xml.

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. 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/.

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. For more information, see http://www.cbp.gov/xp/cgov/trade/legal/informed_compliance_pubs/.

Trade Trends is produced biannually and features graphical analysis and trade highlights. While U.S. Census Bureau has been producing monthly trade statements at the aggregate level, this report is designed to trace major trade patterns and their impact on CBP workload and initiatives, as defined in the "CBP Trade Strategy". For more information, visit http://www.cbp.gov/xp/cgov/trade/trade_outreach/trade_strategy/.

Travel Facilitation

Border Entry Wait Times Customs and Border Protection's (CBP) RSS feeds of border wait times make it easier to view air and land border wait times through a desktop RSS reader as well as on electronic devices, such as smart phones. For more information, visit http://apps.cbp.gov/bwt/.

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, visit https://apps.cbp.gov/eallegations/, or contact the Commercial Targeting and Enforcement, Office of International Trade at: (800) BE-ALERT.

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

Global Entry, one of the CBP trusted traveler programs, allows pre-approved, low-risk travelers expedited clearance upon arrival into the U.S. 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, visit www.globalentry.gov, apply online at https://goes-app.cbp.dhs.gov/, or contact cbp.goes.support@dhs.gov (866) 530-4172.

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

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, at train stations, or crossing U.S. borders. To initiate an inquiry, log onto the DHS TRIP website, www.dhs.gov/trip. For more information, contact the TSA Contact Center, (866) 289-9673.

Trusted Traveler Programs (TTP) provide expedited travel for pre-approved, low risk travelers through dedicated lanes and kiosks upon arrival in the U.S. These programs include NEXUS, SENTRI, FAST (for commercial drivers), and Global Entry. NEXUS, SENTRI, and FAST program members receive technology-enabled credentials while Global Entry members use their passport. All of the programs facilitate border processing by confirming membership, identity, and running law enforcement checks. For more information about trusted traveler programs, visit http://www.cbp.gov/xp/cgov/travel/trusted_traveler/.

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.

Western Hemisphere Travel Initiative (WHTI) requires citizens of the U.S., Canada, and Bermuda to present a passport or other acceptable document that denotes identity and citizenship when entering the U.S. For more information about WHTI, visit http://www.getyouhome.gov/, or contact CBP Customer Service at (877)227-5511 or (703) 526-4200, TDD: (866) 880-6582.

Enforcing and Administering Our Immigration Laws

Virtually all Americans are affected by our immigration system. A fair and effective immigration system enriches American society, unifies families, and promotes our security. Conversely, persistent problems in immigration policy can consume valuable resources needed to advance other security objectives, undermine confidence in the rule of law, and make it harder to focus on the most dangerous threats facing our country. In short, the success of our Nation's immigration policy plays a critical role in advancing homeland security, and our overall homeland security policy must be implemented in a manner that supports an immigration system that succeeds in advancing American interests.

CIS Ombudsman

CIS Ombudsman Annual Reports to Congress 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. For more information, see http://www.dhs.gov/xabout/structure/gc_1183996985695.shtm.

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

CIS Ombudsman's Community Call-In Teleconference Series provides an opportunity to discuss your interactions with 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.

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. Recommendations for process changes should not only identify the problem experienced, but should also contain a proposed solution that will not only benefit an individual case, but others who may be experiencing the same problem as well. Send comments, examples, and suggestions to cisombudsman@dhs.gov.

Submit a Case Problem to the CIS Ombudsman If you are experiencing problems during the adjudication of an immigration benefit with 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). For more information, see http://www.dhs.gov/files/programs/editorial_0497.shtm.

Immigration

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. For more information, see http://www.uscis.gov/USCIS/Office%20of%20Citizenship/Citizenship%20Resource%20Center%20Site/Publications/PDFs/M-677.pdf.

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

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

USCIS Information for Employers and Employees is a website regarding the employment authorization verification process and the immigration petition process. Please visit www.uscis.gov and click on 'Information for Employers and Employees' under 'Working in the US' or

click here. For more information contact Public.Engagement@dhs.gov.

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

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

Immigration Enforcement

Carrier Liaison Program (CLP) provides standardized training and assistance to international air carriers related to admissibility and fraudulent document detection in order to encourage carrier compliance with U.S. immigration laws. For more information about CLP, visit http://www.cbp.gov/xp/cgov/travel/inspections_carriers_facilities/clp/, or contact CLP@dhs.gov 621-7817.

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

E-Verify is an Internet-based system that allows an employer, using information reported on an employee Form I-9, to determine eligibility to work in the U.S. 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 searchable web pages, demonstration videos, guides on employee rights and employer responsibilities, fact sheets, weekly webinars, an overview presentation, brochures and posters for employers and employees. USCIS also has speakers and trainers available to give live presentations at conferences and meetings across the country. For more information, see http://www.dhs.gov/everify or contact E-Verify@dhs.gov, (888) 464-4218.

Form I-9, Employment Eligibility Verification is a form that U.S. employers and their new hires have been required to complete since November 6, 1986. Completion of the form shows that the employer has examined documentation from each newly hired employee to verify his or her identity and eligibility to work in the U.S. Available resources include a Form I-9 webpage, the M-274 Handbook for Employers, Instructions for Completing Form I-9, and the How Do I Complete Form I-9, Employment Eligibility Verification? For more information, see http://www.uscis.gov or call (888) 464-4218.

ICE Mutual Agreement between Government and Employers (IMAGE) Program is a joint government and private sector voluntary initiative that enhances employer compliance and corporate due diligence through training and sharing best practices regarding hiring practices. The goal of IMAGE is for the government to work with employers to develop a more secure and stable workforce and restore the integrity of the U.S. immigration system. For more information, see www.ice.gov/image or contact IMAGE@dhs.gov.

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

Student and Exchange Visitor Program (SEVP) was established in 2003 as the DHS front line effort to ensure that the student visa system is not exploited by those wishing to do harm to the United States. SEVP collects, maintains, and shares information in accordance with applicable laws and DHS policies so that only legitimate foreign students or exchange visitors gain entry to the U.S. The result is an easily accessible information system that provides timely information to the Department of State, Department of Justice, U.S. Customs and Border Protection, U.S. Citizenship and Immigration Services, and ICE. For more information, visit http://www.ice.gov/sevis/ or contact the SEVP Response Center at (703) 603-3400.

Verification Programs Videos are available to help employers use E-Verify in a non-discriminatory manner and in full compliance with their responsibilities under the terms of use. The videos provide invaluable information to human resources personnel. An employer video, Employee Responsibilities and Worker Rights, showcases model employer behavior and emphasizes an employer responsibility to use E-Verify properly, and in a manner that respects worker rights. A separate video, Employer Rights and Responsibilities, available in English and Spanish, emphasizes worker rights when employers use E-Verify, and worker responsibilities when contesting mismatches. The videos emphasize proper treatment of workers, and contain vignettes addressing a worker mismatch. The videos, produced jointly by the CRCL and USCIS are available online at www.uscis.gov/everify.

Written pamphlets accompany the videos and serve as helpful desktop reminders. You may order (at no cost) the DVD videos and written pamphlets by contacting the DHS Office for Civil Rights and Civil Liberties at crcl@dhs.gov.

Safeguarding and Securing Cyberspace

Our economic vitality and national security depend today on a vast array of interdependent and critical networks, systems, services, and resources. We know this interconnected world as cyberspace, and without it we cannot communicate, travel, power our homes, run our economy, or obtain government services. Its benefits are tremendous.
Yet as we migrate ever more of our economic and societal transactions to cyberspace, these benefits come with increasing risk. For this reason, safeguarding and securing cyberspace has become one of the homeland security community's most important missions.

Cybersecurity Assessment Tools

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

Cybersecurity Evaluation Program (CSEP) conducts voluntary cybersecurity assessments across all 18 CIKR sectors, within State governments and large urban areas. CSEP affords CIKR sector participants a portfolio of assessment tools, techniques, and analytics, ranging from those that can be self-applied to those that require expert facilitation or mentoring outreach. The CSEP works closely with internal and external stakeholders to measure key performances in cybersecurity management. The Cyber Resiliency Review is being deployed across all 18 Critical Infrastructure Sectors, State, local, Tribal, and Territorial governments. For more information, visit www.dhs.gov/xabout/structure/editorial_0839.shtm or contact CSE@dhs.gov.

Cybersecurity 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 for download or in DVD format. To learn more or download a copy, visit http://www.us-cert.gov/control_systems/satool.html. To obtain a DVD copy, send an e-mail with your mailing address to CSET@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 (ICS) 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.

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

Cybersecurity Incident Resources

Cyber Investigation Section (CIS) In response to an increase in the scope and volume of fraud being perpetrated and facilitated via the internet, the Secret Service developed CIS to coordinate and provide analytical support to the local field offices. CIS is comprised of three components: Analysis & Exploitation Unit, Cyber Operations Unit, and Cyber Intelligence Unit. The CIS focuses on the identification of networks, malware and significant network intrusions. The Analysis and Exploitation Unit focuses on access device fraud, identification fraud, money laundering, and related financial crimes being facilitated through online media. Also included under this unit are analysts and Criminal Research Specialists who focus on foreign language websites, money laundering activities, and digital/electronic currency. For more information, see www.secretservice.gov/ectf.shtml.

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

Cyber Forensics the products developed through this program are cyber forensic analysis devices used by law enforcement in the daily investigation of criminal and terrorist activity and the tools developed allow investigators to visualize, analyze, share, and present data derived from cell phones, GPS devices, computer hard drives, networks, personal data assistants, and other digital media. For more information, contact SandT-CyberLiaison@hq.dhs.gov.

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

National Computer Forensics Institute (NCFI) Is the result of a partnership between the Secret Service and the State of Alabama. The goal of this facility is to provide a national standard of training on a variety of electronic crimes investigations. This program will offer State and local law enforcement officers the training necessary to conduct computer forensics examinations, respond to network intrusion incidents, and conduct basic electronic crimes investigations. The NCFI will also train prosecutors, and judges on the importance of computer forensics to criminal investigations. This training acts as a force multiplier for the Secret Service and other federal law enforcement agencies, thus reducing the volume of cyber crime cases impacting the federal judicial process. For more information, see www.ncfi.usss.gov.

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

U. S. Computer Emergency Readiness Team (US-CERT) 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.

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

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

Cybersecurity Technical Resources

Cybersecurity 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.

Cybersecurity Research and Development Center (CSRDC) DHS S&T utilizes CSRDC to focus cyber security research and development efforts and to involve the best practices and personnel from academic, private industry, Federal and national laboratories. The CSRDC was established by DHS in 2004 to develop security technology for protection of the U.S. cyber infrastructure. For more 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/ or contact SandT-Cyber-Liaison@hq.dhs.gov.

Cybersecurity in the Retail Subsector Webinar provides retail employees and managers with an overview of the cyber threats and vulnerabilities facing the industry. The webinar also reviews the types of cyber systems and infrastructure used by the retail industry and steps that retail personnel can take to address the unique vulnerabilities to those cyber resources. The webinar is available on HSIN-CS at https://connect.hsin.gov/p78334832/. For more information contact CFSTeam@hq.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 or contact US-CERT at info@us-cert.gov (888) 282-0870.

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.

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

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.

Cybersecurity Education and Workforce Development Program (CEWD) fosters effective cybersecurity education and workforce development programs by facilitating the availability of professionals qualified to support the Nation's cybersecurity needs. To support national cybersecurity workforce development, 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. For more information, see http://www.us-cert.gov/ITSecurityEBK/.

Cybersecurity in the Retail Sector Webinar provides retail employees and managers with an overview of the cyber threats and vulnerabilities facing the industry. Viewers will gain a heightened sense of the importance of strengthening cybersecurity in the retail workplace. The webinar also will review the types of cyber systems and infrastructure used by the retail industry and steps that retail personnel can take to address the unique vulnerabilities to those cyber resources. For more information, please contact the Commercial Facilities SSA at CFSTeam@hq.dhs.gov.

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. For more information, contact CSSP@dhs.gov.

Domain Name System Security Extensions (DNSSEC) Deployment Coordinating Initiative provides 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 website contains articles, published research papers, DNSSEC tools, case studies, workshop information and presentation materials. See http://www.dnssec-deployment.org/.

Information Technology Sector Specific Plan (IT SSP) outlines 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 Cyber Alert System offers a variety of information including Technical Cybersecurity Alerts and Bulletins, or more general-interest pieces such as Cybersecurity Alerts and Tips for users with varied technical expertise. For more information, visit http://www.uscert.gov/cas/alldocs.htm or contact info@us-cert.gov (888) 282-0870.

Network Security Information Exchange (NSIE) The NCS and the National Security Telecommunications Advisory Committee (NSTAC) recommended the establishment of an Industry-Government partnership to reduce the vulnerability of the Nations' telecommunications systems to electronic intrusion. The NCS and NSTAC formed separate Government and Industry Network Security Information Exchanges to share ideas on technologies and techniques for addressing and mitigating the risks to the public network and its supporting infrastructures. For more information, visit http://www.ncs.gov/nstac/reports/fact_sheet/NSTAC_08.pdf.

The Protected Repository for the Defense of Infrastructure against Cyber Threats (PREDICT) facilitates 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. 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. For more information visit https://www.predict.org or contact PREDICT-contact@rti.org.

Roadmap to Secure Control Systems in the Chemical Sector describes a plan for voluntarily improving cybersecurity in the Chemical Sector. Chemical Sector stakeholders, government agencies, and asset owners and operators can use this to plan with a common set of goals and objectives. To obtain a copy of the roadmap or for more information, contact ChemicalSector@dhs.gov.

The Top 25 Common Weakness Enumerations (CWE) In cooperation with the System Administration, Audit, Network Security (SANS) Institute, SwA and MITRE issued the report, "Improve Security and Software Assurance: Tackle the CWE Top 25 – The Most Dangerous Programming Errors." The Top 25 CWEs represent the

most significant exploitable software constructs that have made software so vulnerable. Communicating and addressing these problematic issues will serve to improve software security, both during development and while in operation. Read more and see the list of "Top 25 CWE Programming Errors" at https://buildsecurityin.us-cert.gov/swa/cwe/.

Cybersecurity in the Emergency Services Sector Webinar is a one-hour overview of the types of cyber systems and infrastructure that the Emergency Services Sector utilizes and address the threats and vulnerabilities to those cyber resources. The webinar is available on the Homeland Security Information Sharing – Critical Sectors (HSIN-CS) Emergency Services Sector Portal. For access and more information, contact ESSTeam@hq.dhs.gov.

Software Assurance (SwA)

Automating Software Assurance Under SwA sponsorship, MITRE, in collaboration with government, industry, and academic stakeholders, is improving the measurability of security through enumerating baseline security data, providing standardized languages as means for accurately communicating the information, and encouraging sharing of this information with users by developing repositories (see Making Security Measurable: http://buildsecurityin.us-cert.gov/swa/measurable.html). MITRE issues electronic newsletters on the following technologies employed in automating SwA: Common Vulnerabilities and Exposures (CVE); Common Weakness Enumeration (CWE); Common Attack Pattern Enumeration and Classification (CAPEC); Open Vulnerability and Assessment Language (OVAL); and Malware Attribute Enumeration and Characterization (MAEC).

Software Assurance Program (SwA) Software Assurance is the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted and that software applications function in the intended manner. Grounded in the National Strategy to Secure Cyberspace, the SwA Program develops practical guidance and tools, and promotes research and development of secure software engineering. Resources including articles, webinars, podcasts, and tools for software security automation and process improvement are constantly updated at the SwA Community Resources and Information Clearinghouse located at https://buildsecurityin.us-cert.gov/swa/. For more information, contact software.assurance@dhs.gov.

Software Assurance (SwA) Forum and Working Group Sessions Four times per year, under the co-sponsorship of organizations in DHS, the Department of Defense (DoD), and the National Institute for Standards and Technology (NIST), the SwA Forum and Working Group Sessions provide a venue for participants to share their knowledge and expertise in software security while interacting and networking with key leaders in industry, government, and academia. The gatherings are unique in focus by bringing together a stakeholder community to protect the Nation's key information technologies, most of which are enabled and controlled by software. The SwA Forum and Working Group Sessions are means for fulfilling the Open Government Initiative, reflecting the three principles of transparency, participation, and collaboration. During the Forums, the SwA Program offers 10 to 12 free tutorials. Several of these tutorials are available on line from the Software Engineering Institute's Virtual Training Environment (VTE) at https://www.vte.cert.org/vteweb/go/3719.aspx.

Software Assurance (SwA) Resources To support SwA in higher education, SwA and the Software Engineering Institute (SEI) have developed Software Assurance Curriculum Materials (https://buildsecurityin.us-cert.gov/swa/mswa.html) which are freely available for download. This curriculum is formally recognized by the Institute of Electrical and Electronics Engineers (IEEE) and the Association for Computing Machinery (ACM). At the Forum and Working Group Sessions, SwA distributes CDs of SwA resources. Included on the CDs are guides, reports, and brochures on numerous topics such as: SwA Capability Benchmarking Documents (https://buildsecurityin.us-cert.gov/swa/proself_assm.html); SwA Ecosystem Page (https://buildsecurityin.us-cert.gov/swa/ecosystem.html); FAQs and Fact Sheets on SwA Forums and Working Groups (https://buildsecurityin.us-cert.gov/swa/faq.html); Whitepapers from the Software Assurance Community (https://buildsecurityin.us-cert.gov/swa/ttpe_research.html); Evaluating and Mitigating Software Supply Chain Security Risk, May 2010 (https://buildsecurityin.us-cert.gov/swa/downloads/MitigatingSWsupplyChainRisks10tn016.pdf); and SwA Pocket Guide Series - free, downloadable documents on critical software assurance topics (https://buildsecurityin.us-cert.gov/swa/pocket_guide_series.html).

Software Assurance (SwA) Email Newsletter provides excellent updates and new information related to the SwA program. To subscribe to the newsletter, email listproc@nist.gov and put 'subscribe' in the subject line and 'subscribe sw.assurance' in the body of the email.

Software Assurance (SwA) Checklist for Software Supply Chain Risk Management SwA developed and deployed the "SwA Checklist for Software Supply Chain Risk Management" which identifies common elements of publicly available software assurance models. The SwA Checklist provides a consolidated view of current software assurance goals and best practices in the context of an organized SwA initiative. The checklist includes mappings between the SwA Checklist practices and practices identified in existing SwA maturity models and related capability maturity models. This mapping provides a valuable reference for those wishing to improve their software assurance capabilities. For more information, see https://buildsecurityin.us-cert.gov/swa/proself_assm.html#checklist.

Software Assurance (SwA) Outreach As part of an extensive outreach effort, SwA participates in conferences and webinars with Information Systems Security Association (ISSA), Open Web Application Security Project (OWASP), and other organizations interested in application security. More about SwA relevant webinars is available on the BSI and CRIC websites. Please visit https://buildsecurityin.us-cert.gov/swa/webinars.html for more information. Moreover, SwA supports online communities of interest, such as the Software Assurance Education Discussion Group on LinkedIn (http://www.linkedin.com/groups?mostPopular=&gid=3430456) and the Software Assurance Mega-Community (http://www.linkedin.com/groups?home=&gid=1776555&trk=anet_ug_hm)

Ensuring Resilience to Disasters

Despite ongoing vigilance and efforts to protect this country and its citizens, major accidents and disasters, as well as deliberate attacks, will occur. The challenge is to build the capacity of American society to be resilient in the face of disruptions, disasters, and other crises. Our vision is a Nation that understands the hazards and risks we face; is prepared for disasters; can withstand the disruptions disasters may cause; can sustain social trust, economic, and other functions under adverse conditions; can manage itself effectively during a crisis; can recover quickly and effectively; and can adapt to conditions that have changed as a result of the event.

Business Preparedness

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.

FEMA Private Sector Division communicates, cultivates and advocates for collaboration between the private sector and FEMA to support FEMA capabilities and to enhance national preparedness, protection, response, recovery, and mitigation of all hazards. Its vision is to establish and maintain a national reputation for effective support to our private sector stakeholders through credible, reliable and meaningful two-way communication. For more information email FEMA-Private-Sector@dhs.gov or visit www.fema.gov/privatesector.

Public Transportation Emergency Preparedness Workshop - Connecting Communities Program brings mass transit and passenger rail agency' 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 to prepare and protect their communities. The two-day workshops enable the participants to apply their knowledge and experiences to a range of security and emergency response scenarios. For more information, see http://www.connectingcommunities.net or contact: MassTransitSecurity@dhs.gov.

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 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 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.

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.

The Technical Assistance (TA) Program builds and sustains capabilities through specific services and analytical capacities. 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 that may be DHS grantees, provide 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 email FEMA-TARequest@fema.gov.

The Voluntary Private Sector Preparedness Accreditation and Certification Program (PS-Prep) enhances nationwide resilience in an all-hazards environment by encouraging private sector preparedness. The program will provide a mechanism by which a private sector entity-a company, facility, not-for-profit corporation, hospital, stadium, university, etc.-can certify that it conforms to one or more preparedness standards adopted by DHS. Participation in the PS-Prep Program is completely voluntary. No private sector entity will be required by DHS to comply with any standard adopted under the program, though DHS encourages all private sector entities to seriously consider seeking certification on one or more standards that will be adopted by DHS. For details about PS Prep see www.fema.gov/privatesector/preparedness.

Emergency Communications

National Emergency Communications Plan (NECP) sets goals and identifies key national priorities to enhance

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

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

National Security Telecommunications Advisory Committee (NSTAC) Recommendations address national security and emergency preparedness issues from a private sector perspective and reflect over a quarter-century of private sector advice to the President and the Nation. Issues include network convergence, network security, emergency communications operations, resiliency and emergency communications interoperability. NSTAC recommendations can be found at http://www.ncs.gov/nstac/nstac_publications.html. For more information, contact nstac1@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. For more information, see http://www.cmasforum.com/ or contact cmasforum@sra.com.

Communications Sector Specific Plan (COMM SSP) involves the National Communications System in partnership with government and private sector communications members to ensure the Nation's communications networks and systems are secure, resilient and rapidly restored after an incident. The COMM SSP utilizes government and industry partnerships to protect the communications infrastructure; adopts approaches to identify risks, coordinate with other critical infrastructure sectors and customers on dependencies and solutions for mitigating risk, and works with DHS to integrate plan outcomes into national critical infrastructure/key resources (CI/KR) products. Communications SSP is available at http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications.pdf. For more information, contact comms_sector@hq.dhs.gov.

Emergency Communications Guidance Documents and Methodologies are stakeholder-driven guidance documents and methodologies to support emergency responders across the Nation as they plan for and implement emergency communications initiatives. These resources identify and promote best practices for improving statewide governance, developing standard operating procedures, managing technology, supporting training and exercises, and encouraging use of interoperable communications. Each is available publicly and is updated as needed. Examples include Establishing Governance to Achieve Statewide Communications Interoperability, and the Formal Agreement and Standard Operating Procedure Template Suite. For more information, contact the Office of Emergency Communications at oec@hq.dhs.gov or visit http://www.dhs.gov/xabout/structure/gc_1189774174005.shtm.

Emergency Data Exchange Language (EDXL) messaging standards help emergency responders exchange critical data, including alerts, hospital capacity, and availability of response personnel and equipment. The National Incident Management System Supporting Technology Evaluation Program (NIMS STEP) evaluates the adherence of products to the EDXL suite of standards. NIMS STEP provides industry with an independent third party evaluation of products, devices, systems, and data management tools – including off-the-shelf hardware and software – that support emergency managers and responders in decision making prior to, and during, emergency operations. Evaluation activities are designed to help expand technology solutions, and provide the emergency management/response community with a comprehensive process to assist in the purchasing of incident management products. For more information on the EDXL standards, see http://www.oasis-open.org and for more information on the NIMS STEP see, http://www.nimsstep.org.

Government Emergency Telecommunications Service (GETS) provides authorized emergency response personnel with the resources to make emergency phone calls by priority queuing through the Nation's public communications networks. By calling the GETS access number and using an assigned PIN, Federal, State, local and Tribal leaders, first responders, and private sector emergency response personnel receive priority queuing – allowing emergency calls to be placed ahead of routine phone traffic. The GETS website provides information on eligibility, technical assistance and administrative assistance for registering, maintaining and using GETS. For more information, see http://gets.ncs.gov, or contact gets@dhs.gov.

INFOGRAMs The Emergency Management & Response-Information Sharing & Analysis Center (EMR-ISAC) was established to provide information services that support the infrastructure protection and resilience activities of all Emergency Services Sector (ESS) departments, agencies, and organizations (public and private) nation-wide. InfoGrams contain four short articles issued weekly about Critical Infrastructure Protection (CIP) and Critical Infrastructure Resiliency (CIR) trends and developments. To acquire a no-cost subscription to EMR-ISAC information, send an e-mail request to emr-isac@dhs.gov; to inquire about the practice of CIP or CIR within an ESS organization, call 301-447-1325.

Multi-Band Radio (MBR) Technology offers the emergency response community an opportunity to improve interoperability across agencies, disciplines, and jurisdictions by providing the capability to communicate on all public safety radio bands. The S&T Office for Interoperability and Compatibility's (OIC) MBR technology project is evaluating this new technology through a series of test demonstrations and pilot evaluations to ensure that equipment meets the user requirements identified by the emergency response community. Upon completion, data and user feedback collected during the test and evaluation phases will be published in a procurement guide that will assist emergency response agencies in identifying equipment functionality offered by various manufacturers that meets their mission requirements. For more information, see http://www.safecomprogram.gov/SAFECOM/currentprojects/mbr/MultiBandRadio.htm and contact sandtfrg@dhs.gov to obtain more information on the public safety user requirements that help inform these pilots.

National Communications System (NCS) Fiscal Year Report provides government agencies, private sector entities and the general public a synopsis on the accomplishments of the NCS during each fiscal year. The report covers the NCS role in emergency response operations, highlights the accomplishments of the Office of the Manager branches, and publishes updates on national security and emergency preparedness communications efforts from the 24 Federal Departments and Agencies that comprise the NCS. NCS Fiscal Year reports can be found at http://www.ncs.gov/library.html. For more information, contact ncsweb1@dhs.gov.

SAFECOM Guidance for Federal Grant Programs outlines recommended allowable costs and applications requirements for Federal grant programs that provide 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/SAFECOM/library/grant/1638_fy2011.htm. For more information, contact the Office of Emergency Communications at oec@hq.dhs.gov.

SAFECOM Program provides communications 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 website provides members of the emergency response community and other constituents with information and resources to help them meet their communications and interoperability needs. The site offers comprehensive information on topics relevant to emergency response communications and features best practices that have evolved from real-world situations. For more information, see http://www.safecomprogram.gov, or contact SAFECOM@dhs.gov.

Telecommunications Service Priority (TSP) Program is a Federal Communications Commission program managed by the National Communications System that registers communications circuits for eligible Federal, State, local, Tribal and private sector entities. By registering these key circuits, eligible agencies will receive priority restoration in the event of a national disaster or emergency. The TSP website provides information on eligibility, technical assistance and administrative assistance for registering circuits for TSP. For more information, see http://tsp.ncs.gov, contact tsp@dhs.gov.

Video Quality in Public Safety (VQiPS) Working Group was formed to focus on the major policy, technology, and practical uses and challenges of public safety video systems. Comprised of emergency responders, academics, Federal partners, and vendors, the Working Group developed an end-user guide to help practitioners articulate their needs to vendors when they look to purchase or upgrade video systems. For more information, 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.

Virtual USA (vUSA), integrates technologies, methodologies, and capabilities for sharing and collaborating using public, multi-jurisdictional, and private sector information for the purpose of protecting lives, property, and the environment. It improves situational awareness, enhances decision-making, and facilitates a common operating view that enables users to enhance their existing systems while maintaining control of their own data. vUSA is improving emergency response by ensuring that practitioners at all levels have immediate access to the information they need to make decisions, when they need it. As part of vUSA, S&T developed a prototype that enables authorized users to share and obtain relevant actionable information in real-time. The vUSA prototype is currently being used by states in the Southeast and Pacific Northwest regions to improve both statewide information-sharing capabilities and regional information sharing capabilities. More information can be found at www.firstresponder.gov.

Voice over Internet Protocol (VoIP) Project researches IP-enabled communication technologies and evaluates promising solutions. This project enables 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. For more information, see http://www.safecomprogram.gov/SAFECOM/currentprojects/voip/ and http://www.pscr.gov/projects/broadband/voip/voip.php, contact VoIP_Working_Group@sra.com.

Wireless Priority Service (WPS) is the sister program to GETS and provides authorized emergency response personnel with the resources to make emergency wireless phone calls by priority queuing through the Nation's public communications networks. Authorized WPS users – using authorized WPS wireless carriers – are granted priority service during national emergencies. Federal, State, local and Tribal leaders, first responders, and private sector emergency response personnel are eligible. The WPS website provides information on eligibility, technical assistance and administrative assistance for registering,

maintaining and using WPS. See http://wps.ncs.gov, contact wps@dhs.gov.

Disaster Response

Area Committees and Area Contingency Plans (ACPs) improve coordination between Federal, State and local authorities and industry, and to strengthen on-scene response to the discharge of oil and hazardous materials. All U.S. critical ports have Area Committees and Area Contingency Plans. See the AMSC, Area Committee and HSC postings at www.homeport.uscg.mil. Each USCG Sector Commander has a port homepage on the USCG Homeport website; interested prospective partners should check their respective port page on Homeport for contact information. Many HSCs also have their own state- or locally-sponsored websites, maintained separately from USCG Homeport.

DisasterAssistance.gov is a secure, web portal that consolidates disaster assistance information. 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 website technical assistance, contact (800) 745-0243.

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.

The Emergency Food and Shelter National Board Program (EFSP) was created in 1983 to supplement the work of local social service organizations, both non-profit and governmental, within the U.S. and its territories, to help people in need of emergency economic assistance. Funding is open to all organizations helping hungry and homeless people. This collaborative effort between the non-profit and public sectors has provided over $3.6 billion in Federal funds during its 28-year history. For more information, visit http://efsp.unitedway.org.

Lessons Learned and Information Sharing (LLIS.gov), 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, visit www.llis.gov, or contact the program via e-mail feedback@llis.dhs.gov, or call (866) 276-7001.

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

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

Disaster Response Laws & Regulations

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

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

FEMA Regulatory Materials 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.

Emergency Responder Resources

Center for Domestic Preparedness (CDP) offers several programs that are designed for those with emergency response and healthcare responsibilities, or who meet the criteria specified in the website mentioned below. CDP offers courses in chemical, biological, radiological, nuclear, and explosive incident response, toxic agent training, and healthcare response for mass casualty incidents, Radiological Emergency Preparedness Program courses, field force operations, and the National Incident

Management System (NIMS). CDP offers interdisciplinary training that includes the opportunity to train in the Nation's only toxic agent training facility dedicated to the civilian response community, the Chemical, Ordnance, Biological, and Radiological Training Facility (COBRATF). The CDP's healthcare courses include exercises in a hospital dedicated solely to preparedness and response training, the Noble Training Facility (NTF). Training provided by the CDP for state, local, and tribal agencies is free of charge; round-trip air and ground transportation, lodging, and meals are provided at no cost to responders or their agency. Federal, private sector, and international agencies are encouraged to attend on a space available basis but they must pay a tuition fee for the courses in addition to transportation, meals and lodging fees. For more information, see http://cdp.dhs.gov/index.html or call (866) 213-9553.

Emergency Services Sector Online Training Catalog describes public and private resources and programs that are applicable to first responders. To obtain access to the online catalog contact the Emergency Services Sector Specific Agency at ESSTeam@hq.dhs.gov.

Emergency Services Sector (ESS) Video This 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.

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. For more information, or to request materials contact the Emergency Services Sector-Specific Agency at ESSTeam@hq.dhs.gov.

First Responder Communities of Practice is an online network of vetted, active, and retired first responders, emergency response professionals and Federal, State, local, or Tribal Homeland Security officials sponsored by the DHS S&T's First Responder Technologies (R-Tech) program. Registered members of this professional network share information, ideas, and best practices, enabling them to more efficiently and effectively prepare for all hazards. See www.firstresponder.gov or https://communities.firstresponder.gov.

FirstResponder.gov is a portal that enables Federal, State, local, and Tribal first responders to easily access and leverage Federal web services, information on resources, products, standards, testing and evaluation, and best practices, in a collaborative environment. The portal provides first responders with information to develop or deploy technologies that would enhance homeland security. For more information, see www.firstresponder.gov.

First Responders 'Go Kit' Training Video is a video designed to demonstrate what first responders should have in their personal and family emergency kit. For more information please contact the Emergency Services SSA at ESSTeam@hq.dhs.gov.

Integrated Pilot Comprehensive Exercise (IPCE) is an FBI led activity, developed in coordination with DHS and the Nuclear Regulatory Commission, to enhance the capabilities of responders to integrate with onsite security personnel in response to a security incident at a nuclear power plant. The initiative is a no-fault training opportunity which culminates in both tabletop and full-scale exercises at a nuclear power plant. For more information, contact NuclearSSA@hq.dhs.gov

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

R-Tech Bulletin is a publication on technologies of interest to first responders who have received funding, in part, from the Federal Government. Interested individuals can subscribe to the bulletin by RSS feed or can download the bulletin at http://www.firstresponder.gov/Pages/Newsletter.aspx.

Ready Responder Program for the Emergency Services Sector Webinar is a one-hour web-based seminar will focus on First Responder preparedness and best practices and how the Ready Responder program contributes to a safer, more secure and more resilient America. The webinar is available on the Homeland Security Information Sharing – Critical Sectors (HSIN-CS) Emergency Services Sector portal. For access and more information, contact the Emergency Services Sector at ESSTeam@hq.dhs.gov.

Technologies for Critical Incident Preparedness (TCIP) Conference and Exposition highlights DOJ, DHS, and DoD technologies; Research, Development, Testing & Evaluation 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. For more information, see http://www.tcipexpo.com.

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

Personal and Community Preparedness

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 plants, and terrorism. For more information see 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.

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.

Community Emergency Response Team (CERT) helps train citizens to better prepare for and respond to emergency situations in their communities. 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.

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, 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.

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. For more information, see www.floodsmart.gov; flood insurance agents, please visit www.agents.floodsmart.gov or e-mail asktheexpert@riskmapcds.com.

Ready.gov is the preparedness resource for your family. Launched in February 2003, Ready is a national public service advertising (PSA) campaign designed to educate and empower Americans to prepare for and respond to emergencies including natural and man-made disasters. Ready and its Spanish language version Listo ask individuals to do three key things: (1) get an emergency supply kit, (2) make a family emergency plan, and (3) be informed about the different types of emergencies that could occur and their appropriate responses. For more information, see www.ready.gov.

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. 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. For more information, see www.fema.gov/government/grant/hma/index.shtm.

U.S. Fire Administration (USFA) Fire Prevention and Safety Campaigns deliver fire prevention and safety education 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.

Preparedness Education

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

DHS Center of Excellence: National Center for the Study of Preparedness and Catastrophic Event Response is improving the Nation's preparedness and ability to respond to disasters through scientific research focused on medical and public health preparedness strategies, response capabilities, and surge capacity. Resources include the Electronic Mass Casualty Assessment and Planning Scenarios, the Triage Tool for Accurate Disposition of Patients in Disaster Response, the Urban Evacuation Model, and the Global Scale Agent Model. For more information, see http://www.pacercenter.org/ or contact universityprograms@dhs.gov.

Emergency Planning Exercises are a series of Tabletop Exercise presentations to advance organizational continuity, preparedness and resiliency. Each exercise is conducted with a realistic disaster scenario and facilitated discussion of how to plan, protect, respond and recover. To learn more or to download the exercises visit http://www.fema.gov/privatesector/exercises.shtm.

FEMA Emergency Management Institute Independent Study Program offers self-paced courses designed for those with emergency management responsibilities, as well as for the general public. The FEMA 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 training courses, please visit http://training.fema.gov/IS/ or contact us (301) 447-1200.

FEMA Emergency Management Institute Programs offers several programs that are designed for those with emergency management responsibilities or meet the criteria specified at the website cited below. The training is free of charge, but individuals from the 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 encourages individuals from the private sector to participate in its courses. EMI programs include, but are not limited to, the Master Trainer Program, Master Exercise Practitioner Program, Professional Development Series, Applied Practices Series and the FEMA 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 U.S. The LRC collection of books and research reports may also be accessed by requesting interlibrary loan through a local library. For more information see http://www.lrc.fema.gov ornetclrc@dhs.gov (800) 638-1821.

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.

National Training and Education Division (NTED) courses are delivered in a variety of formats including web-based, resident, and non-resident. For more information, visit www.firstrespondertraining.gov or contact askCSID@dhs.gov (800) 368-6498.

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 review and final approval of all neighborhood 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 review and recommend changes to 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.

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.

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	
CBP	Trusted Traveler Programs (NEXUS, SENTRI, FAST)	Cbp.goes.support@dhs.gov	
CRCL	Training	crcltraining@dhs.gov	(202) 357-8258
CRCL	Disability Preparedness	Disability.preparedness@dhs.gov	(202) 357-8483
CRCL	Contact	CRCLOutreach@dhs.gov	
CRCL	Complaints	crcl@dhs.gov	(202) 401-1474; (866) 644-8360
DHS	Center for Faith-based & Neighborhood Partnerships	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 Public Affairs		(202) 282-8010
DHS	Office of Small and Disadvantaged Business Utilization		(202) 447-5555
DHS	Private Sector Office	Private.sector@dhs.gov	(202) 282-8484
DHS	Privacy Office	Privacy@dhs.gov	(703) 235-0780
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) 267-2591
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	SEVP@DHS.gov	(703) 603-3400
NPPD/CS&C	Control Systems Security Program (CSSP)	CSSP@dhs.gov	
NPPD/CS&C	Cybersecurity Evaluation Tool	CSET@dhs.gov	
NPPD/CS&C	Information Technology Sector	ncsd_cipcs@hq.dhs.gov	
NPPD/CS&C	Office of Emergency Communications	oec@hq.dhs.gov	

NPPD/CS&C	SAFECOM Program	SAFECOMGovernance@dhs.gov	
NPPD/CS&C	Software Assurance Program	software.assurance@dhs.gov	
NPPD/CS&C	U.S. Computer Emergency Readiness Team (US-CERT)	info@us-cert.gov	(888) 282-0870
NPPD/CS&C	US-CERT Secure Operations Center	soc@us-cert.gov	(888) 282-0870
NPPD/IP	Chemical Facility Anti-Terrorism Standards (CFATS) Help Desk	cfats@dhs.gov	(866) 323-2957
NPPD/IP	Chemical Facility Anti-Terrorism Standards Compliance Assistance Visit Requests	CFATS@dhs.gov	
NPPD/IP	Chemical Sector Specific Agency	ChemicalSector@dhs.gov	
NPPD/IP	CIKR Asset Protection Technical Assistance Program (CAPTAP)	Traininghelp@hq.dhs.gov	(703) 235-3939
NPPD/IP	Commercial Facilities Sector-Specific Agency	CFSteam@hq.dhs.gov	
NPPD/IP	Critical Manufacturing Sector-Specific Agency	criticalmanufacturing@hq.dhs.gov	
NPPD/IP	Dams Sector-Specific Agency	dams@dhs.gov	
NPPD/IP	Emergency Services Sector-Specific Agency	ESSTeam@hq.dhs.gov	
NPPD/IP	Infrastructure Data Taxonomy (IDT)	IDT@hq.dhs.gov	
NPPD/IP	Integrated Common Analytical Viewer (iCAV)	iCAV.info@hq.dhs.gov	(703) 235-4949
NPPD/IP	IP Education and Learning Series	IP_Education@hq.dhs.gov	
NPPD/IP	National Infrastructure Coordination Center (NICC)	NICC@dhs.gov	(202) 282-9201
NPPD/IP	National Infrastructure Protection Plan (NIPP)	NIPP@dhs.gov	(703) 603-5069
NPPD/IP	Nuclear Sector-Specific Agency	nuclearSSA@hq.dhs.gov	
NPPD/IP	Office for Bombing Prevention	OBP@dhs.gov	(703) 235-5723
NPPD/IP	Protected Critical Infrastructure Information (PCII) Program	pcii-info@dhs.gov	(202) 360-3023
NPPD/IP	Protective Security Advisor (PSA) Field Operations Staff	fobanalysts@hq.dhs.gov	(703) 235-9349
NPPD/IP	Sector Specific Agency Executive Management Office	SSAexecsec@dhs.gov	
NPPD/IP	Vulnerability Assessments Branch	IPassessments@dhs.gov.	
NPPD/IP	Sector Coordinating Council	Sector.Partnership@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	Cyber Security Liaison	SandT-Cyber-Liaison@hq.dhs.gov	
S&T	Office of University Programs	universityprograms@dhs.gov	(202) 254-5695
S&T	Project 25 Compliance Assessment Program (P25 CAP)	P25CAP@dhs.gov	
S&T	SAFETY Act	SAFETYActHelpDesk@dhs.gov	(866) 788-9318
S&T	Small Business Innovation Program (SBIR)	stsbir.program@dhs.gov	
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
USCG	America's Waterway Watch	aww@uscg.mil	
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	
USSS	Office of Investigations		(202) 406-5716
USSS	Criminal Investigative Division		(202) 406-9330
USSS	Forensic Services Division		(202) 406-5926

Appendix B – Index

A

B

C

D

E

F

G

H

I

N

P

R

S

T

W