Preventing Terrorism and Enhancing Security

Protecting the American people from terrorist threats is our founding principle and our highest priority. The Department of Homeland Security's counterterrorism responsibilities focus on three goals: prevent terrorist attacks; prevent the unauthorized acquisition, importation, movement, or use of chemical, biological, radiological, and nuclear materials and capabilities within the United States; and reduce the vulnerability of critical infrastructure and key resources, essential leadership, and major events to terrorist attacks and other hazards.

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/sites/default/files/assets/pdf/Intermodal/nonssi_acstl_8_2_oct11_12.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, 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 an emergency scenario. For more information, see http://www.viterbi.usc.edu/aviation/.

Aviation Security Advisory Committee (ASAC) provides advice and recommendations for improving aviation security measures to the Administrator of the Transportation Security Administration. The committee was initially established in 1989 following the destruction of Pan American World Airways Flight 103 by a terrorist bomb. The ASAC has traditionally been composed of members representing key constituencies affected by aviation security requirements. Subcommittees include Air Cargo, International Aviation, General Aviation, Risk-Based Security, and Passenger Advocacy. For more information, see http://www.tsa.gov/aviation-security-advisory-committee.

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 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/stakeholders/programs-and-initiatives-1#Air%20Cargo%20Watch.

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/stakeholders/airspace-waivers-0 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/stakeholders/training-and-exercises-0.

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

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 http://www.tsa.gov/certified-cargo-screening-program or contact ccsp@dhs.gov or the TSA Contact Center, 866-289-9673.

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/stakeholders/security-programs-and-initiatives or contact MDThree@dhs.gov.

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/stakeholders/security-programs-and-initiatives.

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://blog.tsa.gov/2009/06/tsa-paperless-boarding-pass-pilot.html 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 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/stakeholders/security-directives.

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/stakeholders/secure-flight-program, 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, it provides 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.

Bombing Prevention

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.

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 improves participants' ability to manage improvised explosive device (IED) threats by outlining specific safety precautions associated with explosive incidents and bomb threats. The Workshop reinforces an integrated combination of planning, training, exercises, and equipment acquisition in order to maximize available resources. Key public and private sector representatives knowledgeable in regional efforts should attend. This Workshop is designed to accommodate 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) Counterterrorism Workshop is a four to eight-hour awareness level Workshop designed to enhance the knowledge of state and local law enforcement and public/private sector stakeholders by providing exposure to key elements of the IED threat, surveillance detection methods and soft target awareness. The Workshop illustrates baseline awareness and prevention actions that reduce vulnerabilities to counter the threat along with collaborating information sharing resources to improve preparedness. This designed approach better enables the owners and operators of critical infrastructure to deter, prevent, detect, protect against, and respond to the potential use of explosives in the United States. This Workshop is designed to accommodate 125 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.

Improvised Explosive Device (IED) Recognition and Detection for Railroad Industry Employees Training (CD) is an eight-hour Workshop which enhances participants' knowledge of improvised explosive device (IED) awareness, prevention measures, and planning protocols by outlining specific search techniques that reduce vulnerability and mitigate the risk of potential IED attacks. The Workshop culminates in a practical application of skills during which participants demonstrate these search techniques while working together as a team. Law enforcement and private sector security personnel responsible for bomb threat management planning and response should attend. This Workshop is designed to accommodate 40 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) Search Procedures Workshop is an eight-hour Workshop which enhances participants' knowledge of improvised explosive device (IED) awareness, prevention measures, and planning protocols by outlining specific search techniques that reduce vulnerability and mitigate the risk of terrorist IED attacks. The Workshop culminates in a practical application of skills during which participants demonstrate these search techniques while working together as a team. Law enforcement and private sector security personnel responsible for bomb threat management planning and response should attend. This Workshop is designed to accommodate 40 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) The Office of Infrastructure Protection's Office for Bombing Prevention and the Commercial Facilities Sector-Specific Agency developed 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 Threat Awareness and Detection, focuses on identifying Improvised Explosive Devices (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, please contact the NPPD/IP Commercial Facilities SSA at CFSTeam@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.

Protective Measures Course is a two-day course designed to provide executive and employee level personnel in the public/private sector with the knowledge to identify the appropriate protective measures for their unique sector. The course focuses on teaching the participants the threat analysis process, terrorist methodology and planning cycle, available protective measures, and determining which protective measures to employ. This course is designed to accommodate 75 participants. To request training, contact your State Homeland Security Advisor; see http://www.dhs.gov/xgovt/editorial_0291.shtm for a current list.

Surveillance Detection for Law Enforcement and Security Professionals is a three-day course designed for law enforcement and private sector security professionals that provides participants with the knowledge, skills, and abilities to detect hostile surveillance conducted against critical infrastructure. The course, consisting of five lectures and three exercises, increases awareness of terrorist tactics and attack history and illustrates the means and methods used to detect surveillance and identify suspicious behavior. This course is designed to 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.

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 CRITICAL INFRASTRUCTURE 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 Coordinating 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=100:1:70962511397808 88. For more information, contact the CFATS Help Desk at CSAT@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_122476691 4427.shtm or contact the CFATS 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 CSAT@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@hq.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 CSAT@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 http://www.dhs.gov/files/programs/gc_1247235870769.shtmor contact CFATS@hq.dhs.gov.

Chemical Security Summit The NPPD/IP's Chemical Sector Specific Agency (SSA) co-hosts the annual Chemical Sector Security Summit with the Chemical Sector Coordinating Council (SCC). The 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 transportation security. Summits also include pre-Summit Demonstrations and post-Summit workshops. For more details on the Summit, please visit www.dhs.gov/chemicalsecuritysummit or contact the NPPD/IP Chemical SSA at ChemicalSector@hq.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@hq.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 (ICS) Security Resource DVD The chemical industry, in partnership with DHS, has collected a wealth of cybersecurity information to assist owners and operators in addressing ICS security. The DVD contains a wide-range of useful information, including: ICS training resources; existing standards; reporting guidelines; cybersecurity tabletop exercises; and the National Cyber Security Division's Cyber Security Evaluation Tool. The DVD is available for free upon request. For more information or to obtain a copy of the DVD, please contact the NPPD/IP Chemical SSA at ChemicalSector@hq.dhs.gov.

Chemical Sector Security Awareness Guide The purpose of this document is to assist 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. For more information, please contact the NPPD/IP Chemical SSA at ChemicalSector@hq.dhs.gov.

Chemical Sector Training Resources Guide The 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 officers to train their employees on industry best practices, physical and cybersecurity awareness, and emergency management and response. For more information, please contact the NPPD/IP Chemical SSA at ChemicalSector@hq.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 http://www.dhs.gov/files/programs/gc_1181835547413.shtm. For more information, contact the CFATS Help Desk at CSAT@dhs.gov 866-323-2957.

Infrastructure Protection Sector-Specific Tabletop Exercise Program (IP-SSTEP), Chemical Sector Tabletop Exercise (TTX) The IP-SSTEP Chemical Sector TTX is an unclassified and adaptable exercise developed to create 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 needed coordination with other entities, both private and government, regarding their facility. It also contains everything needed for a company or facility to conduct a Homeland Security Exercise and Evaluation Program (HSEEP) compliant TTX. For more information, please contact the NPPD/IP Chemical SSA at ChemicalSector@hq.dhs.gov.

Know Your Customer DHS and the FBI cooperated to create a flyer for use as a communication tool for chemical companies' marketing, sales, purchasing and product stewardship personnel, who could encounter suspicious inquiries about poisonous chemicals and gases either directly or indirectly. The flyer strongly encourages chemical companies, suppliers, manufacturers, customers, distributors, and transportation service providers to continue increasing employee awareness of these risks in their organization, reviewing management practices for sensitive materials, and reporting suspicious activities.

For more information or to obtain a copy of the flyer, please contact the Chemical SSA at ChemicalSector@hq.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@hq.dhs.gov.

Security Seminar & Exercise Series for Chemical Industry Stakeholders This 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 towards the specific interests of the organizing entity and can include a wide-variety of topics and security scenarios such as an active shooter, a hostage situation, a suspicious package, or a Vehicle Borne improvised explosive device (VBIED). For more information or to obtain a list of scheduled events, please contact the NPPD/IP Chemical SSA at ChemicalSector@hq.dhs.gov.

Voluntary Chemical Assessment Tool (VCAT) VCAT is a secure, web-based application and self-assessment tool originally 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. For more information, please contact the NPPD/IP Chemical SSA at ChemicalSector@hq.dhs.gov.

Web-Based Chemical Security Awareness Training Program The training program is an interactive tool available free to chemical facilities nationwide to increase security awareness. The training is designed for all facility employees, not just those traditionally involved in security. Upon completion, a certificate is awarded to the student. To access the training, please visit https://chemicalsecuritytraining.dhs.gov/. For more information, please contact the NPPD/IP Chemical SSA at ChemicalSector@hq.dhs.gov.

Who's Who in Chemical Sector Security This document describes the roles and responsibilities of different DHS components with relation to Chemical Security. For more information, or to obtain the report, please contact the NPPD/IP Chemical SSA at ChemicalSector@hq.dhs.gov.

Critical Infrastructure – Multiple Sectors

Active Shooter Resources include a desk reference guide, a reference poster, and a pocket-sized 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. The desk reference guide, pocket card and poster are available on the following websites, also available in Spanish translation. http://www.dhs.gov/xlibrary/assets/active_shooter_poster.pdf, http://www.dhs.gov/xlibrary/assets/active_shooter_booklet.pdf, http://www.dhs.gov/xlibrary/assets/active_shooter_pocket_card.pdf, http://www.dhs.gov/xlibrary/assets/active-shooter-poster-spanish.pdf, http://www.dhs.gov/xlibrary/assets/active-shooter-pocket-spanish.pdf. For more information, please contact the Commercial Facilities SSA at CFSTeam@dhs.gov.

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.

Critical Infrastructure Asset Protection Technical Assistance Program (CAPTAP) is a weeklong course designed to assist state and local law enforcement, first responders, emergency managers, 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 mapping and geospatial tool. For more information, see www.dhs.gov/files/programs/gc_1195679577314.shtm or contact TrainingHelp@hq.dhs.gov.

Critical Infrastructure Protection and Resilience Toolkit is intended to be a starting point for small and medium sized businesses to integrate infrastructure protection and resilience into preparedness, risk management, business continuity, emergency management, security, and other related disciplines. For more information, contact IP_Education@hq.dhs.gov.

Critical Infrastructure Learning Series The Learning Series allows NPPD/IP to provide information and online seminars on current and emerging critical infrastructure topics to critical infrastructure owners and operators, government partners and others. Register for updates at http://www.dhs.gov/ciwebinars.

Critical Infrastructure Partnership Advisory Council Supply Chain Working Group (SCWG) The SCWG was established to serve as a Government and industry forum to discuss the existing and evolving supply chain risks to the Communications Sector. The SCWG's objective is to enhance Government's awareness of industry transactions of interest and best practices relevant to telecommunications supply chain risk management. Through this voluntary information sharing framework, SCWG members aim to develop a program that addresses Federal Government concerns for national security and primary mission essential function integrity, while delivering valuable information and guidance to private sector partners. For more information, contact will.williams@hq.dhs.gov.

Critical Infrastructure Resource Center is an online tool designed to build awareness and understanding of the scope and efforts of all of the18 critical infrastructure sectors. Each sector page provides Sector goals, priorities, protective programs, and initiatives, and other resources, as reflected in the latest Sector-Specific Plans and Sector Web pages. To access the Resource Center: http://training.fema.gov/EMIWeb/IS/IS860a/CIRC/index.htm.

Critical Infrastructure Training Module provides an overview of the National Infrastructure Protection Plan (NIPP) and critical infrastructure 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 Infrastructure Sector Snapshots provide a quick look at SOPD sectors and generally contain sector overviews; information on sector partnerships; information on critical infrastructure protection issues and priority programs. For more information, see http://www.dhs.gov/xlibrary/assets/nipp_annrpt.pdf. For more information, contact NIPP@dhs.gov.

Cross-Sector Active Shooter Security Seminar and Exercise Workshop This is a one-day workshop designed to be applicable for any sector for general awareness of how to respond to an active shooter incident. The workshop will enhance awareness of an active shooter event by educating participants on the history of active shooter events; describing common behavior, conditions, and situations associated with active shooters. The intent of the program is to foster communication between critical infrastructure owners and operators and local emergency response teams by discussion of interoperability, communications, and best practices for planning, preparedness and response during a facilitated tabletop exercise. For more information or to obtain a list of scheduled events, please contact the Sector Outreach and Programs Division at ASworkshop@hq.dhs.gov.

The Cutting Edge Tools Resilience Program Website was created under the platform of the DHS Science and Technology Directorate's High Performance and Integrated Design Program to improve the security and resilience of our Nation's buildings and infrastructure. The website has manuals, software and tools to better prepare buildings and infrastructure to recover from manmade and natural disaster events such as explosive blasts; chemical, biological, and radiological (CBR) agents; floods; hurricanes; earthquakes, and fires. For more information see www.dhs.gov/bips.

Dealing with Workplace Violence Tabletop Exercise (TTX) The Office of Infrastructure Protection's (IP) Sector Outreach and Programs Division has developed the Dealing with Workplace Violence Tabletop Exercise (TTX) that focuses on an active-shooter situation in the workplace. The TTX is broken up into three modules: the pre-incident phase, including recognizing potential warning signs of workplace violence; the incident and response phase; and the assessment phase. The TTX will focus discussion on how to limit escalation and reduce the threat of violent behavior, but in the event that an incident does occur, it also addresses how facilities can work with their employees, and public and private partners to ensure they are prepared and able to recover from an event as quickly as possible. For more information, please contact the Sector Outreach and Programs Division at SOPDExecSec@dhs.gov.

FoodSHIELD is a Web-based system for communication, coordination, community-building, education, and training among the nation's food and agriculture sectors. FoodSHIELD enables real-time response and decision making by facilitating collaborations between public health and food regulatory officials at the local, state, and federal levels. FoodSHIELD currently has registered participation from labs and regulatory agencies in all 50 states. As a rapidly maturing infrastructure, more than 190 workgroups actively use FoodSHIELD to plan, coordinate, and develop new strategies for food defense and protection. More than 64,000 minutes are logged each month using our core webinar capabilities allowing easy collaboration amongst stakeholders and participants across the sector. Impressively, many of these workgroup participants represent different agencies and states providing for the first time true collaboration and coordination capabilities across federal and state boundaries. For more information, please visit www.foodshield.org.

DHS Center of Excellence: Global Terrorism Database is an open-source database including information on terrorist events around the world from 1970 through 2011 (with additional updates planned for the future). In addition to the GTD, the world's largest unclassified dataset on terrorism incidents, the START consortium makes many other datasets available to advance research and analysis on the topics of terrorism, counterterrorism, and community

resiliency. For more information, see www.start.umd.edu/gtd and http://www.start.umd.edu/start/data_collections/ or universityprograms@hq.dhs.gov.

DHS Center of Excellence: 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 Consortium for the Study of Terrorism and Responses to Terrorism (START) advances science-based knowledge about the human causes and consequences of terrorism as a leading resource for security professionals. START will provide security professionals with objective data and the highest quality, data-driven research findings terrorism and closely related asymmetric threats, counterterrorism and community resiliency in an effort to ensure that homeland security policies and operations reflect these understandings about human behaviors. For more information, see www.start.umd.edu or universityprograms@hq.dhs.gov.

DHS YouTube Critical Infrastructure Videos A number of short video webisodes are available on the DHS YouTube Channel. The webisodes include Joint Operations Centers, Critical Infrastructure Interdependencies, Special Event Preparedness, Critical Infrastructure Protection and Reducing Vulnerabilities. DHS YouTube Channel: Resource Guide SOPD Current: 18 Sept 2012 http://www.youtube.com/playlist?list=UUpkaznWj_9PIVgO0BRKXu8w&feature=plcp.

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.

The Joint Counterterrorism Awareness Workshop Series (JCTAWS) is a nationwide initiative designed to improve the ability of local jurisdictions to prepare for, protect against, and respond to complex coordinated terrorist attacks. JCTAWS, held across the country, brings together Federal, state, and local participants representing law enforcement, fire, emergency medical services, communication centers, private sector and non-governmental communities to address this type of threat. The workshop is designed to emphasize tactical operational response, medical care under fire, hospital surge and treatment for an incident more commonly seen on the battlefield than in an urban setting. Specifically, the workshop underscores the need for a whole community response and aims to: review existing preparedness, response and interdiction plans, policies, and procedures related to a complex coordinated terrorist attack; improve situational awareness and encourage information sharing among all stakeholders in the event of a complex coordinated terrorist attack; and identify and share best practices and lessons learned for tactical response and medical preparedness. After each JCTAWS, the host city receives a summary report. The report includes key findings from the workshop; addresses the city's capability gaps and potential mitigation strategies; and provides a list of resources to address the gaps. The JCTAWS interagency planning group (NCTC/DHS/FBI) conducts a follow-up meeting with each city to determine if further guidance and assistance are needed. For more information, contact FEMA-Private-Sector@fema.dhs.gov or private.sector@hq.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.

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.

NPPD/IP SOPD Critical Infrastructure Sector Snapshots, Fact Sheets and Brochures These two-page snapshots provide a quick look at each of the eighteen sectors and generally contain sector overviews; information on sector partnerships; critical infrastructure protection challenges; and priority programs. For more information, see http://www.dhs.gov/files/programs/gc_1189168948944.shtm."

NPPD/IP Training Page The landing page provides links to a wide array of cross-sector and sector-specific no-cost training programs and resources which are available to private sector partners. The Web-based and classroom courses provide government officials and critical infrastructure owners and operators with the knowledge and skills needed to implement critical infrastructure protection and resilience activities. Access the Training Programs for Infrastructure

Partners Page on DHS.gov: http://www.dhs.gov/files/training/training-critical-infrastructure-partners.shtm.

Protective Security Advisors (PSAs) are DHS/NPPD/IP infrastructure security experts deployed across the country who serve 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 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 PSCDOperations@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.

Critical Manufacturing

Critical Manufacturing Cybersecurity Tabletop Exercise In partnership with Critical Manufacturing Sector Coordinating Council members and the DHS National Cyber Security Division (NCSD) exercise program, the Critical Manufacturing SSA has developed a cybersecurity tabletop exercise to highlight potential cybersecurity vulnerabilities. This exercise is divided into two modules focusing on threats to business systems and industrial control systems. This unclassified tabletop exercise is easily deployable and can be administered by an organization's IT personnel. For more information, please contact the Critical Manufacturing SSA at CriticalManufacturing@hq.dhs.gov.

Critical Manufacturing Security Conference The Critical Manufacturing Security Conference features various vendors and presenters pertinent to the manufacturing arena. Designed for industry professionals throughout the sector, this event provides an important opportunity for Critical Manufacturing Sector security partners to engage in meaningful dialogue and share ideas to enhance sector security. For more information, contact CriticalManufacturing@dhs.gov.

Critical Manufacturing Partnership Road Show This program provides Critical Manufacturing Sector members an opportunity to participate in onsite visits to various DHS locations. The visits include briefings on current threats to the U.S., including to the Critical Manufacturing Sector and related infrastructure. For more information, email CriticalManufacturing@dhs.gov.

SOPD/TSA Joint Exercise Program This program allows Critical Manufacturers to develop advanced tabletop exercises that determine gaps and mitigate vulnerabilities in their respective transportation supply chains within the U.S. and cross border (particularly Canada and Mexico). 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, please contact the NPPD/IP Critical Manufacturing SSA at CriticalManufacturing@hq.dhs.gov.

Commercial Facilities

Active Threat Recognition for Retail Security Officers This 85-minute presentation discusses signs of potential 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. Also includes One-pager/factsheet. For more information, please contact the Commercial Facilities SSA at CFSTeam@dhs.gov.

Commercial Facilities Sector Pandemic Planning Documents These 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 Venue Manager's Academy for Venue Safety and Security. For more information, please contact the Commercial Facilities SSA at CFSTeam@dhs.gov.

DHS Retail Video: "What's in Store – Ordinary People/Extraordinary Events" The Department of Homeland Security's, Infrastructure Protection's Partnership and Outreach Division, Office for Bombing Prevention and the Commercial Facilities Sector-Specific Agency created a multimedia training video for retail employees of commercial shopping venues to alert them of the signs of suspicious behavior in the workplace. 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/list?media_type=vi

deo&year_filter[value][year]=&month_filter[value][year]=&month_filter[value][month]=&title=&items_per_page=25. For more information, please contact the NPPD/IP Commercial Facilities SSA at CFSTeam@dhs.gov.

DHS Sports Leagues/Public Assembly Video: "Check It! How to Check a Bag" Designed to raise the level of awareness for front line facility employees by highlighting the indicators of suspicious activity, this video provides information to help employees properly search bags in order to protect venues and patrons across the country. For more information, please contact the NPPD/IP Commercial Facilities SSA at CFSTeam@dhs.gov.

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.

Hotel and Lodging Advisory Poster This 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 was designed in tandem with the Commercial Facilities SCC and the Lodging Subsector and is available at http://www.dhs.gov/xlibrary/assets/ip_cikr_hotel_advisory.pdf. For more information, please contact the NPPD/IP Commercial Facilities SSA at CFSTeam@dhs.gov.

Infrastructure Protection Sector-Specific Table Top Exercise Program (SSTEP) for the Commercial Facilities Retail/Lodging Subsectors and Sports Leagues/Public Assembly Subsectors These tools are unclassified, adaptable and immediately deployable exercises which focus 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 action 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, please contact the NPPD/IP Commercial Facilities SSA at CFSTeam@dhs.gov.

IS-906 Workplace Security Awareness This online training provides guidance to individuals and organizations on how to improve security in the workplace. The course promotes workplace security practices applicable across all 18 critical infrastructure sectors. Threat scenarios include: Access & Security Control, Criminal & Suspicious Activities, Workplace Violence, and Cyber Threats. The training may be accessed on the Federal Emergency Management Agency Emergency Management Institute Web site: http://training.fema.gov/EMIWeb/IS/IS906.asp. For more information about Office of Infrastructure Protection training courses, please contact: IP_Education@hq.dhs.gov.

IS-907 Active Shooter: What You Can Do This online training provides guidance to individuals, including managers and employees, so that they can prepare to respond to an active shooter situation. The 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; 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 Federal Emergency Management Agency Emergency Management Institute Web site: http://training.fema.gov/EMIWeb/IS/IS907.asp. For more information about Office of Infrastructure Protection training courses, please contact: IP_Education@hq.dhs.gov .

IS-912 Retail Security Awareness: Understanding the Hidden Hazards This online training increases awareness of persons involved in commercial retail operations of the actions they can take to identify and report suspicious purchases or thefts of products that could be used in terrorist or other criminal activities. The course provides an overview of steps to identify and monitor high-risk product inventories and reporting suspicious activities to law enforcement agencies. The course is designed for retail managers, loss prevention specialists, risk management specialists, product managers, sales associates and others involved in retail operations. The training may be accessed on the Federal Emergency Management Agency Emergency Management Institute Web site: http://training.fema.gov/EMIWeb/IS/IS912.asp. For more information about Office of Infrastructure Protection training courses, please contact: IP_Education@hq.dhs.gov.

Lodging Video: "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.

Mountain Resorts and Outdoor Events Protective Measures Guides These guides are a compilation of

materials shared by industry leaders which are intended for reference and guidance purposes only. They provide an overview of protective measures that can be implemented to assist owners and operators of commercial facilities in planning and managing security at their facilities or at their events, as well as examples of successful planning, organization, coordination, communication, operations, and training activities. For more information, please contact the Commercial Facilities SSA at CFSTeam@dhs.gov.

Protective Measures Guide for U.S. Sports Leagues This Protective Measures Guide 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 Sector-Specific Agency at CFSteam@hq.dhs.gov.

Protective Measures Guide for the U.S. Lodging Industry Produced in collaboration with the American Hotel & Lodging Association (AH&LA), the Protective Measures Guide for the U.S. Lodging Industry offers options for hotels to consider when implementing protective measures. This guide provides an overview of threat, vulnerability, and protective measures designed to assist hotel owners and operators in planning and managing security at their facilities. For more information, please contact the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

Retail and Shopping Center Advisory Poster helps train retail employees on the recognition of suspicious behavior and how to report it. For more information, contact the Commercial Facilities SSA at CFSTeam@hq.dhs.gov.

Risk Self-Assessment Tool for Stadiums and Arenas, Performing Art Centers, Lodging, Convention Centers, Racetracks, and Theme Parks The Risk Self Assessment Tool (RSAT) is a secure, Web-based application designed to assist managers of public assembly facilities 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. It is also accompanied by a Fact Sheet/Brochure. For more information, please contact the NPPD/IP Commercial Facilities SSA at CFSTeam@dhs.gov or RSAT@hq.dhs.gov.

Sports Venue Bag Search Procedures Guide This guide provides suggestions for developing and implementing bag search procedures at sporting event venues hosting major sporting events. The purpose for establishing bag search procedures is to control items which are hand carried into the sports venue. The bag search procedures should be a part of the venue's over all Security Plan and should be tested and evaluated as stated in the Security Plan. The actual implementation of bag search procedures and level of search detail will depend upon the threat to the venue as determined by the venue's security manager. For more information, please contact the Commercial Facilities SSA at CFSTeam@dhs.gov.

Sports Venue Credentialing Guide This guide provides suggestions for developing and implementing credentialing procedures at sporting event venues that host professional sporting events. The purpose for establishing a credentialing program is to control and restrict access to a sports venue, and provide venue management with information on those who have access. Credentialing can also be used to control and restrict vehicle movement within a venue. For more information, please contact the Commercial Facilities SSA at CFSTeam@dhs.gov.

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.

Dams Security

Active and Passive Vehicle Barriers Guide (Dams Sector) This guide provides owners/operators with information on a variety of active and passive vehicle barriers, and properly designing and selecting vehicle barrier systems. For more information, please contact the NPPD/IP Dams SSA at Dams@hq.dhs.gov.

Common Risk Model for Dams (CRM-D) describes a model for estimating risk to dams and navigation locks located across the United States. The model was funded and guided by the United States Army Corps of Engineers (USACE) and is currently being developed as a on-line tool through ANL as a part of the Dams Sector Analysis Tool (DSAT). The model incorporates commonly used risk metrics that are designed to be straightforward, transparent, and mathematically defensible. The methodology was piloted in the second half of 2011 at nearly 20 different USACE facilities. For more information, please contact the Dams SSA at Dams@hq.dhs.gov.

Comprehensive Facility Reports (CFR). These reports on Dams Sector critical assets 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@hq.dhs.gov.

Consequence-Based Top Screen Fact Sheet This fact sheet provides information pertaining to the Consequence-Based Top Screen (CTS) methodology, including how it was developed, its primary purpose, and the Web-based tool with which it is implemented. For more information, see http://www.dhs.gov/files/programs/gc_1260541882284.shtm or contact the NPPD/IP Dams SSA at Dams@hq.dhs.gov.

Dams and Energy Sector Interdependency Study Examines the interdependencies between two critical infrastructure sectors—Dams and Energy—with a particular emphasis on the variability of weather patterns and competing demands for water, which determine the amount of water available for hydroelectric power generation. For more information, please contact the Dams SSA at Dams@hq.dhs.gov.

Dams Sector Analysis Tool (DSAT) is an integrated data management system and dams-specific analysis tool that establishes an integrated analysis gateway for all Dams Sector-related tools and information, which allows for a single source for data input and analysis. In addition, DSAT provides access to simplified dam break flood inundation analysis capabilities through the Decision Support System for Water Infrastructural Safety (DSS-WISE), developed by the National Center for Computational Hydroscience and Engineering at the University of Mississippi. For more information, contact the Dams SSA at dams@hq.dhs.gov.

Dams Sector Consequence-Based Top Screen (CTS) Tool The purpose of the CTS methodology is to identify 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. It is also accompanied by Fact Sheet/Brochure. For more information, please contact the NPPD/IP Dams SSA at Dams@hq.dhs.gov.

Dams Sector Consequence-Based Top Screen (CTS) Reference Guide The user-guide provides information on the methodology, how it was developed, its primary purpose, and the Web-based tool with which it is implemented. For more information, please contact the NPPD/IP Dams SSA at Dams@hq.dhs.gov.

Dams Sector Crisis Management Handbook Provides 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://www.damsafety.org/media/Documents/Security/DamsSectorCrisisManagementHandbook.pdf. For more information, please contact the NPPD/IP Dams SSA at Dams@hq.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@hq.dhs.gov.

Dams Sector Roadmap to Secure Control Systems provides a comprehensive framework and recommended strategies focused on the protection of industrial control systems across the Dams Sector in order to enhance the sector's understanding and management of cyber risks; facilitate the identification of practical risk mitigation solutions; promote information sharing; and improve sector-wide awareness of cyber security concerns. For more information, please contact the NPPD/IP Dams SSA at Dams@hq.dhs.gov.

Dams Sector Security Awareness Guide This is a non-FOUO version of the Dam Sector Security Awareness Handbook for 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 NPPD/IP Dams SSA at Dams@hq.dhs.gov.

Dams Sector Security Awareness Guide – Levees This guide assists levee owners in identifying security concerns, coordinating proper response, and establishing effective partnerships with local law enforcement and first responder communities. For more information, please contact the Dams SSA at Dams@hq.dhs.gov.

Dams Sector Suspicious Activity Reporting Fact Sheet This 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, please contact the Dams SSA at Dams@hq.dhs.gov.

Dams Sector Tabletop Exercise Toolbox (DSTET) – This tool 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. Multiple videos and examples are included as part of the tool for use

during the exercise as "scene-setters." The toolbox includes several modules, which can be tailored to accommodate specific needs at a given facility. The toolbox will assist owners and responders in reviewing information sharing and coordination activities when dealing with a security incident and supports the identification of potential opportunities for improvement, thus enhancing overall incident response planning. The toolbox includes planner instructions, facilitator briefing slides and handbook, situation manual, sample invitation letters, sample feedback forms, and exercise reference materials. For more information, please contact the NPPD/IP Dams SSA at Dams@hq.dhs.gov.

Dams Sector Waterside Barriers Guide Provides owners/operators with information on waterside barriers and their use, maintenance, and effectiveness; elements that must be carefully taken into consideration when selecting waterside barriers. For more information, please contact the NPPD/IP Dams SSA at Dams@hq.dhs.gov.

Dams Sector 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@hq.dhs.gov.

Emergency Preparedness Guidelines for Levees: A Guide for Owners and Operators Assists public and private stakeholders that have responsibilities as owners or operators in managing levees, floodwalls, pumping stations, and any other components of flood risk management systems. For more information, please contact the Dams SSA at Dams@hq.dhs.gov.

Estimating Economic Consequences for Dam Failure Scenarios provides information describing the economic consequence estimation approaches most commonly used in the U.S., and discusses their advantages and limitations. For more information, please contact the Dams SSA at Dams@hq.dhs.gov.

Estimating Loss of Life for Dam Failure Scenarios Provides information describing the loss of life estimation approaches most commonly used in the U.S. and Canada, and discusses their advantages and limitations. For more information, please contact the Dams SSA at Dams@hq.dhs.gov.

IS-870 Dams Sector: Crisis Management Overview is Web-based training focused on information provided within the Dams Sector Crisis Management handbook. To access this course visit: http://training.fema.gov/EMIWeb/IS/is870.asp. For more information, please contact the NPPD/IP Dams SSA at Dams@hq.dhs.gov.

IS-871 Dams Sector: Security Awareness (FOUO) This Web-based training focuses on information provided within the Dams Sector Security Awareness handbook. To access this course visit: http://training.fema.gov/EMIWeb/IS/is871.asp. For more information, please contact the NPPD/IP Dams SSA at Dams@hq.dhs.gov.

IS-872 Dams Sector: Protective Measures (FOUO) This Web-based training focuses on information provided within the Dams Sector Protective Measures handbook. To access this course visit: http://training.fema.gov/EMIWeb/IS/is872.asp. For more information, please contact the NPPD/IP Dams SSA at Dams@hq.dhs.gov.

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

Physical Security Measures for Levees Brochure provides information on physical security measures that a levee owner could employ and the factors affecting the selection of those measures. The brochure is available at http://www.dhs.gov/dams-sector-publications-training-and-resources. For more information please contact the Dams SSA at Dams@hq.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@hq.dhs.gov.

Security Awareness for Levee Owners Brochure This brochure provides succinct information on surveillance indicators and incident reporting. The brochure is available at http://www.dhs.gov/dams-sector-publications-training-and-resources. For more information, please contact the NPPD/IP Dams SSA at Dams@hq.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@hq.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@hq.dhs.gov.

Suspicious Activity Reporting Tool is a standardized means by which critical infrastructure stakeholders can report suspicious or unusual activities to the government via sector portals on the Homeland Security Information Network-Critical Sectors (HSIN-CS). Reports submitted to the tool are reviewed by the National Infrastructure Coordinating Center

(NICC), shared with appropriate government recipients, redacted and posted to HSIN-CS. Email HSINCS@dhs.gov to request access to HSIN-CS.

Security Awareness for Levee Owners Brochure provides information on surveillance indicators and incident reporting. For more information, see https://www.dhs.gov/files/programs/gc_1283878065033.shtm or contact the Dams SSA at Dams@hq.dhs.gov.

Food Safety and Influenza

DHS Center of Excellence: Center for Advancing Microbial Risk Assessment (CAMRA), co-led by Michigan State University and Drexel University and established jointly with the U.S. Environmental Protection Agency, 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 Zoonotic and Animal Disease Defense (ZADD) 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, The Biosecurity Research Institute (BRI) 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://www.ceezad.org 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.

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 NPPD/IP developed sector-specific guides for pandemic influenza for the Chemical, Commercial Facilities, Dams, Emergency Services, and Nuclear Sectors. For more information, please contact the NPPD/IP Sector Outreach and Programs Division at SOPDExecSec@dhs.gov.

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/stakeholders/documents-and-reports-0. 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/stakeholders/trucking-hazmat. 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/stakeholders/trucking-hazmat. 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/stakeholders/trucking-hazmat or contact highwaysecurity@dhs.gov.

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

Land Transportation and Pipeline

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: 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. 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/stakeholders/trucking-hazmat 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 Office of Security Policy and Industry Engagement (OSPIE) 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/i-step 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/stakeholders/documents-and-reports-0 or contact highwaysecurity@dhs.gov.

Land Transportation Antiterrorism Training Program (LTATP) is an effort by the Federal Law Enforcement Training Center to enhance knowledge, skills, and capabilities of law enforcement and security officials to prevent acts of terrorism. 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: FLETC-CounterterrorismDivision@hq.dhs.gov.

On the Tracks Rail Sabotage Awareness and Reporting (DVD & Poster) Training to provide those responsible for the safety and security of our rail system with information on the nature of rail sabotage threats and the necessary steps to take in safeguarding against its execution. The video addresses where to look for potential sabotage threats, the categories of threats to be on alert for, and the steps to take in reporting objects or activities that appear out of the ordinary. This information reinforces the important role of front-line employees, who have firsthand knowledge and experience working in the field every day, in helping to deter a terrorist attack on the rail system. For more information, contact freightrailsecurity@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/stakeholders/motorcoach or contact highwaysecurity@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/stakeholders/training-and-exercises. For more information contact the Pipeline Security Division at PipelineSecurity@dhs.gov.

Protecting Pipeline Infrastructure: The Law Enforcement Role is a DVD intended to enhance the law enforcement community's understanding of pipeline systems and their security issues. The DVD provides a basic understanding of how pipeline systems function, the principle products they transport, and includes a discussion of the threats and vulnerabilities to pipelines. The primary audience for this DVD is local, state, and federal law enforcement, federal security partners, and others involved with infrastructure security. Viewers should come away with a better understanding of the typical measures taken to protect pipelines and actions they can take to assist pipeline operators during times of heightened security alert. For more information and to request a copy, see http://www.tsa.gov/stakeholders/pipeline-security

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) training provides school bus drivers, school 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. For more information, see http://www.tsa.gov/stakeholders/school-transportation-security-awareness, or contact highwaysecurity@dhs.gov.

Transportation Security Grant Program (TSGP) 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 http://www.fema.gov/government/grant/tsgp/ or contact askcsid@dhs.gov, 800-368-6498.

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/sites/default/files/assets/pdf/Intermodal/hwmc_annual_report_2006.pdf.

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://aww.aww-sp.com/Americas_Waterway_Watch/Home.html or

contact aww@uscg.mil 877-24WATCH (877-249-2824).

Area Committees and Area Contingency Plans (ACPs) improve coordination between federal, state and local authorities and industry, and strengthen on-scene response to the discharge of oil and hazardous materials. 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. All U.S. critical ports have Area Committees and Area Contingency Plans. See the AMSC, Area Committee and HSC postings at https://homeport.uscg.mil/mycg/portal/ep/home.do.

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 http://www.uscg.mil/hq/cg5/cg544/amsc.asp, http://www.law.cornell.edu/cfr/text/33/103.305, or https://homeport.uscg.mil/mycg/portal/ep/home.do.

Area Maritime Security Plans (AMSPs) are coordination and communication plans that align all levels of government (Federal, State, tribal, territorial, and local) and private industry port partners to prevent, protect against, respond to, and initial recovery from a transportation security incident. The 43 AMSPs cover each of the Nation's Captain of the Port Zones. Facilities and ports must implement security measures as outlined in their approved security plans. The Maritime Security (MARSEC) Level (of which there are three) is set by the Commandant of the Coast Guard to reflect the prevailing threat environment to marine elements of the national transportation system. For more information, see https://homeport.uscg.mil/mycg/portal/ep/home.do.

Area Maritime Security Plans (AMSPs) are exercised annually through the Coast Guard's **Area Maritime Security Training and Exercise Program (AMSTEP)** These interagency, multi-jurisdictional exercises encourage important interaction among maritime stakeholders, including AMSCs, and enable effective cooperation and preparation for maritime security contingencies. AMSTEP exercises help stakeholders maintain and evaluate their ability to implement the jointly developed AMSPs. Stakeholders include Federal agencies, State, local, territorial and tribal governments, and private sector partners, and may include facility and vessel security personnel. For more information, see https://homeport.uscg.mil/mycg/portal/ep/home.do.

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. 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.

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 Disaster Response Intelligent System (DRIS), Coupled Wave/Storm Surge Prediction Model, Storm Surge Forecasting Tool, In-Situ Scour Evaluation Probe, MUNICIPAL Critical Infrastructure Decision Support Tool, and Youth Coping Response Inventory Tool. For more information, visit http://coastalhazardscenter.org/.

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.

Industry Risk Analysis Model (IRAM) is an unclassified version of the Maritime Security Risk Analysis Model (MSRAM). IRAM is available to industry partners to conduct a local risk assessment of their own facilities and vessels applying the same criteria employed by USCG Port Security Specialists (PSS) with MSRAM. IRAM provides a baseline risk analysis capability for owners/operators and assists in rank ordering terrorism-related targets/scenarios, evaluating owner/operator security impact on risk, and developing management strategies to reduce risk. IRAM is managed by the MSRAM program manager. For more information, contact MSRAMHelp@uscg.mil

Harbor Safety Committees, or similar bodies, 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 other maritime stakeholders. Harbor Safety Committees frequently include participation from their respective Captain of the Port. 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, recreational boaters, marine patrols, government, and public or private environmental organizations. For more information, see the AMSC, Area Committee and HSC postings at https://homeport.uscg.mil/mycg/portal/ep/home.do then select "Ports and Waterways," or visit www.harborsafetycommittee.blogspot.com.

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), International Port Security Program, marine safety, maritime domain awareness and information sharing, maritime security, and waterways, regulations/administrative adjudications, vessel standards, counter-piracy, Port Security Advisors, Maritime Transportation Security Act (MTSA), Marine Safety Center, Mariner Credential Verification, and Mariner Credential Application Status. For more information, see https://homeport.uscg.mil/mycg/portal/ep/home.do.

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", "Crowd Control for Passenger Vessels and Terminals", "Maritime Terrorism and Hijacking Situations", "Terminal and Shipboard Evacuation", and "Basic Screening Procedures for Maritime Transportation Security". To order, contact TSA Port & Intermodal Security Division at Maritime@dhs.gov or 571-227-3556.

Maritime Security Risk Analysis Model (MSRAM) is a terrorism risk management tool and process used to conduct scenario-based risk assessments against critical infrastructure, key assets, and targets within each US Coast Guard Captain's of the Port area of responsibility. The execution of the MSRAM process is built upon the assessments and judgments made by Coast Guard field commanders across the country in close partnerships with regional Area Maritime Security Committees, which include maritime industry security professionals. The resultant extensive national dataset contains risk evaluations of a wide array of scenarios for all of the significant assets operating in the U.S. maritime domain. MSRAM offers a dynamic analysis interface capable of generating tailored results and supports operational, tactical and strategic decisions. For more information, contact MSRAMHelp@uscg.mil.

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.

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. 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/port-security-grant-program or contact askcsid@dhs.gov 800-368-6498.

The Port State Information Exchange (PSIX) system contains vessel specific information derived from the United States Coast Guard's Marine Information Safety and Law Enforcement System (MISLE). The information contained in PSIX represents a weekly snapshot of Freedom of Information Act (FOIA) data on U.S. flag vessels, foreign vessels operating in U.S. waters, and Coast Guard contacts with those vessels. Information on open cases or cases pending further action is considered privileged information and is excluded from the PSIX system until the relevant cases are complete and closed. PSIX can be accessed at the following link: http://cgmix.uscg.mil/PSIX/Default.aspx

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/stakeholders/transportation-worker-identification-credential-twic%C2%AE, or contact 866-347-8942.

U.S. Coast Guard Auxiliary is the uniformed volunteer component of the United States Coast Guard. 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. 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

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, freightrailsecurity@dhs.gov, or 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. Membership to the Public Transit portal is provided once vetted by portal administrators. For more information, contact MassTransitSecurity@dhs.gov.

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/transit-security-grant-program 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. For more information, 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. 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. 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 potential 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. 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. For more information, visit http://www.tsa.gov/stakeholders/building-security-force-multipliers or contact 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/sites/default/files/publications/pdf/grants/6th_2009_ibsgp_security_emergency_preparedness_plan_template.pdf 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, contact the Freight Rail Branch at frieghtrailsecurity@dhs.gov.

Nuclear Security

The Domestic Nuclear Detection Office (DNDO) is a jointly staffed agency within the Department of Homeland Security. DNDO is the primary entity in the U.S. government for implementing domestic nuclear detection efforts for a managed and coordinated response to radiological and nuclear threats, as well as integration of federal nuclear forensics programs. Additionally, DNDO is charged with coordinating the development of the global nuclear detection and reporting architecture, with partners from federal, state, local, and international governments and the private sector. DNDO will also develop, acquire, and support the domestic nuclear detection and reporting system. DNDO's Commercial First Initiative will facilitate this by shifting the focus from government development of materiel solutions to a commercial first approach that will leverage industry innovation and facilitate the deployment of detection equipment to DHS components and federal, state, and local stakeholders. For more information, see www.dhs.gov/xabout/structure/editorial_0766.shtm or contact dndo.info@dhs.gov.

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

The Illicit Trafficking Radiation Assessment Program+10 (ITRAP+10), is a partnership between the Domestic Nuclear Detection Office (DNDO) and the European Commission's Joint Research Center (EC/JRC) in Ispra, Italy. ITRAP +10 is designed to assist National organizations to effectively detect radiological materials, whether during the importation, exportation, or shipment in transit. ITRAP+10 provides federal stakeholders and their governmental and commercial partners with an open, objective and reliable data set on the performance of commercially available radiation detection and identification equipment that was collected against the requirements set forth by national and international consensus standards. For more information, contact dndo.info@hq.dhs.gov.

The Joint Analysis Center (JAC) Program provides an interagency coordination mechanism and central monitoring point for the Global Nuclear Detection Architecture (GNDA), maintains situational awareness across the GNDA – to include status of radiological and nuclear (rad/nuc) detection assets, visibility into the status of rad/nuc alarms, awareness of rad/nuc-related incidents and events, data, and trend analyses supporting GNDA operations. The JACCIS, an Information Technology (IT) system specifically developed to support JAC operations, is a secure web application and database which supports alarm adjudication, analysis, information sharing, and reporting for the Global Nuclear Detection Architecture (GNDA) by DNDO and its mission partners. Through its relationship to the National Labs and members of the IC Community, the JAC Program provides technical expertise toward specific requirements of DNDO to include the development of classified annexes for architectural studies; creation of GNDA visualization tools; operations support activities and the ongoing development and execution of red teaming and assessment activities. For more information, see http://www.dhs.gov/xabout/structure/editorial_0766.shtm.

Monthly Unclassified Threat Briefing The NPPD/IP Nuclear SSA holds an unclassified security teleconference for nuclear facility owners and operators, plant managers, and security professionals on the first Wednesday of every month. The teleconference provides the opportunity for the Department of Homeland Security's Office of Intelligence and Analysis and Office for Bombing Prevention to brief the Nuclear Sector on significant changes to the threat environment, results of recent terrorism investigations, and other reported suspicious

incidents and for the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) to brief the Nuclear Sector on recent cyber alerts and advisories. The teleconference also covers significant changes to the threat environment, results of recent terrorism investigations, and other reported suspicious incidents. For more information, please contact the NPPD/IP Nuclear SSA at NuclearSSA@hq.dhs.gov.

National Nuclear Forensics Expertise Development Program (NNFEDP) aims to provide a stable foundation from which to develop and sustain the nuclear forensics workforce. This interagency program is dedicated to maintaining a vibrant academic pathway from undergraduate to post-doctorate study in disciplines directly relevant to nuclear forensics, such as radiochemistry, geochemistry, nuclear physics, nuclear engineering, materials science, and analytical chemistry. The NNFEDP promotes a unique interdisciplinary approach that encourages collaboration among academic programs, universities, and the DOE national laboratories. Initiatives include undergraduate outreach and scholarships; graduate fellowships, internships, and mentoring; post-doctorate fellowships; university education awards; and junior faculty awards. For more information, see http://scuref.org, http://www.dhs.gov/blog/2012/08/28/supporting-next-generation-nuclear-forensic-scientists or contact dndo.info@dhs.gov.

Nuclear Sector Classified Threat Briefing The NPPD/IP Nuclear SSA coordinates both regularly scheduled and incident-specific classified briefings for cleared sector partners. For more information, please contact the NPPD/IP Nuclear SSA at NuclearSSA@hq.dhs.gov.

Nuclear Sector Information Sharing Standard Operating Procedure (SOP) This document is designed to enhance the effectiveness of voluntary information coordination and distribution among members of the Nuclear Sector Information Sharing Environment (ISE). The information-sharing processes are developed as suggested practices and must be used in conjunction with, and subordinate to, legal, regulatory, and industry standard processes that are established within and recognized by the Nuclear Sector and its industry and government members. For more information, please contact the NPPD/IP Nuclear SSA at NuclearSSA@hq.dhs.gov.

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 Security Awareness Guide This document will assist Nuclear Sector owners and operators in their efforts to improve security at their facility, reaffirm awareness of the security risks to the sector, and provide a list of activities or actions that they can take to reduce that risk. For more information, please contact the NPPD/IP Nuclear SSA at 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.

Open Access to ANSI N42 Series Standards DNDO sponsors the Institute of Electrical and Electronics Engineers (IEEE) to provide copies of the ANSI N42 radiation detection standards free of charge to anyone who wants a copy. Visit the web site to obtain the latest published version of one of the sponsored standards is: http://standards.ieee.org/about/get/

Radiological Emergency Preparedness Program (REP) 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 more information, visit http://www.fema.gov/about/divisions/thd_repp.shtm.

Training, Exercise, and Assistance (TE&A) Program TE&A consists of three separately managed but heavily integrated programs and embodies the Domestic Nuclear Detection Office's (DNDO) principal efforts to develop the most effective operational Radiological and Nuclear Detection (RND) practices throughout the Global Nuclear Detection Architecture (GNDA). TE&A, working in collaboration with its federal, state, local, and tribal partners, as well as industry and the national laboratories, identifies best practices and develops the appropriate training and exercise materials to ensure standards-based application of these practices in the field. The Training Program works to break down approved operational concepts into teachable tasks, conditions, and standards at appropriate echelons of the GNDA. Through this process, it develops training products and systems required to meet desired standards, and it makes them available to users enabling them to meet their GNDA-based responsibilities. The Exercise Project develops Homeland Security Exercise Evaluation Program (HSEEP) compliant, operational exercise templates tailored specifically for the GNDA and for federal, state and local programs. The Exercise Project develops exercises standards designed to ensure operational concepts are put to rigorous and realistic examination. This standards-based approach serves as an RND exercise force multiplier that improves the overall domestic exercise efficiency and consistency across the GNDA. The Assistance Program is designed to provide guidance to GNDA partners on how to plan, develop, manage, evaluate, and sustain a RND program. As such, it works directly with federal, state, local, and tribal multi-jurisdictional, multi-disciplinary policy makers, program managers, operational administrators, and subject matter experts to design and implement RND programs and enhance detection capabilities as a means to implement the GNDA. To accomplish this, the Assistance Program provides a system of standardized processes and a suite of scalable tools which allow state and local agencies to develop, implement, and enhance their own

radiological and nuclear detection programs. These tools provide comprehensive guidance for Planning, Organizing, Equipping, Training, and Exercise (POETE) Operations. In other words, they provide a structure for the administration of a domestic preventive RND program and are intended to allow federal, state, local, and tribal agencies develop and implement tailorable, scalable programs while staying true to the framework of the GNDA. For more information, see http://www.dhs.gov/xabout/structure/editorial_0766.shtm.

Who's Who in DHS Nuclear Sector Infrastructure Protection This product describes the roles and responsibilities of DHS components as they relate to the Nuclear Sector. For more information, please contact the NPPD/IP Nuclear SSA at NuclearSSA@hq.dhs.gov.

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 IPassessments@hq.dhs.gov.

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, visit http://www.tsa.gov/stakeholders/advancing-security-baseline or contact MassTransitSecurity@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. 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 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 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 critical infrastructure sectors and sub-sectors; and establish sector baseline security survey scores. Private sector owners and operators interested in an ECIP Visit should contact PSCDOperations@hq.dhs.gov or 703-235-9349.

DHS Center of Excellence: Risk Analysis and Decision Support with: Homeland Security Analysis, Modeling, Integrated, Secured Environment and Repository for Decision Support (HS-ANALISER) . HS-ANALISER (formerly the Risk Analysis Workbench (RAW)) is the National Center for Risk and Economic Analysis of Terrorism Events (CREATE) 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/2008/05/the_risk_analysis_workbench_ra_2.html or contact universityprograms@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 owners and operators interested in receiving more information on the RRAP should contact IPassessments@hq.dhs.gov.

Regional Resiliency Assessment Program (RRAP) Discussion Based Exercises These exercises are offered to those jurisdictions participating in the RRAP. The core component of these efforts will be a capstone Tabletop Exercise (TTX) delivered in approximately the one-year post-Resiliency Analysis delivery timeframe. The core objective of this TTX will be to determine changes to a jurisdiction's/sector's overall Resiliency Baseline due to the implementation of suggested protective measures highlighted by the RRAP process. In the intervening year, Readiness works with the RRAP exercise planning team to deliver other requested preparatory activities, such as workshops, to help shape the capstone TTX. For more information, please

contact the Sector Outreach and Programs Division at SOPDExecSec@dhs.gov.

Sector-Specific Tabletop Exercise Program (SSTEP) This tool allows critical infrastructure partners to develop interactive, discussion-based exercises for their communities of interest, be it at the sector or a facility level. The SSTEP allows users to leverage pre-built exercise templates and tailor them to their communities' specific needs in order to assess, develop, and update plans, programs, policies and procedures within an incident management functional area. For more information, please contact the Sector Outreach and Programs Division at SOPDExecSec@dhs.gov.

Site Assistance Visits (SAVs) Site Assistance Visits 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 a SAV report, protected as 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 IPassessments@hq.dhs.gov.

Special Event and Domestic Incident Tracker (SEDIT) is a web-based tool used by field-deployed personnel to enhance steady state, special event, and domestic incident support capabilities. SEDIT utilizes security and resilience data from Enhanced Critical Infrastructure Protection security surveys and Site Assistance Visits to calculate a Baseline Risk for each critical infrastructure. Integrating reported vulnerabilities, consequences, and threat ratings, the Baseline Risk allows for the prioritization of the Nation's critical infrastructure and key resources. For more information, contact PSCDOperations@hq.dhs.gov or 703-235-9349.

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 collect, prioritize, analyze, and visualize critical infrastructure to prepare, prevent, respond, 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.

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. For more information, see http://www.dhs.gov/files/programs/editorial_0542.shtm or contact CIKR.ISE@dhs.gov 202-312-3421.

DHS Center of Excellence: National Center for Visualization and Data Analytics (CVADA) 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 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.

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".

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.

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) HSIN-CS is the primary information-sharing platform between the critical infrastructure sector stakeholders. With a library of products that increases on an average of every 2 hours, HSIN-CS enables federal, state, local and private sector 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. To request access to HSIN-CS, please contact CIKRISEAccess@hq.dhs.gov. When requesting access, please indicate the critical infrastructure sector to which your company belongs and include your name, company, official email address, and supervisor's name and phone number.

"If You See Something, Say Something™" Campaign In July 2010, the Department of Homeland Security (DHS) launched its national "If You See Something, Say Something™" public awareness campaign – a simple and effective program to raise public awareness of indicators of terrorism and violent crime, and to emphasize the importance of reporting suspicious activity to the proper state and local law enforcement authorities. The campaign was originally used by New York's Metropolitan Transportation Authority (MTA), which has licensed the use of the slogan to DHS for anti-terrorism and anti-crime efforts. For more information, see http://www.dhs.gov/files/reportincidents/see-something-say-something.shtm.

Identity Management enhances security by improving authentication for persons to enable seamless and secure interactions among federal, state, local, and private sector stakeholders ensuring that they have comprehensive, real-time, and relevant information. Through this research, financial and other private sector businesses are able to streamline and strengthen the identity verification process reducing the risks of identity fraud. For more information, please contact SandT-Cyber-Liaison@hq.dhs.gov.

Information Sharing Snapshot This two-page snapshot describes the Information Sharing Environment (ISE). The ISE is designed to improve the overall effectiveness of information sharing between and among federal, state, local, tribal, and territorial governments and the private sector. To enable the protection of critical infrastructure, the Department of Homeland Security established an information-sharing network that is guided primarily by the National Infrastructure Protection Plan (NIPP) and works in coordination with the efforts of the Federal ISE. For more information, see http://www.dhs.gov/xlibrary/assets/NIPP_InfoSharing.pdf.

Infrastructure Data Taxonomy (IDT) Critical infrastructure 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 Critical infrastructure 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 Information Collection System (IICS) is a secure, web-based application designed to provide authorized users 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. For more information, contact IICD-IICS@hq.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.

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 HSINCS@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 202-282-9881.

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. 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 the 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.

The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) Program Management Office (PMO) initiated operations in March 2010 with the challenge of ensuring that regardless of where in the country suspicious activity is reported, these potential indicators of terrorist activity can be analyzed and compared to other SAR information nationwide. The NSI incorporates the informal processes that traditionally exist within law enforcement agencies into the standards, policies, and processes developed by the NSI that allow law enforcement agencies to easily share information with the critical partners that need it to help prevent potential terrorist attacks. For more information, see http://nsi.ncirc.gov/default.aspx.

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, tribal 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. 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.

Suspicious Activity Reporting for Critical Infrastructure Tool This tool is a standardized means by which critical infrastructure stakeholders can report suspicious or unusual activities to the government via sector portals on the Homeland Security Information Network-Critical Sectors (HSIN-CS). Reports submitted to the tool are reviewed by the National Infrastructure Coordinating Center (NICC), shared with appropriate government recipients, redacted and posted to HSIN-CS. To request access to HSIN-CS, please contact HSINCS@dhs.gov.

SOPD Classified Threat Briefings SOPD coordinates both regularly scheduled and incident-specific classified briefings for cleared sector partners. For more information, contact Sector Outreach & Programs Division at SOPDExecSec@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, as well as information about the resources available for timely reporting of suspicious activities. The live webinar is available for download on

Homeland Security Information Network-Critical Sectors (HSIN-CS). For more information, contact SDAWARE@hq.dhs.gov.

Technical Resources 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 https://www.tripwire.dhs.gov/IED/appmanager/IEDPortal/IEDDesktop?_nfpb=true&_pageLabel=LOGIN.

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.

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.

Unified Incident Command and Decision Support (UICDS) is a national "middleware foundation" designed to support information sharing for the National Response Framework and the National Incident Management System, including the Incident Command System. UICDS middleware is transparent to system operators during operations and requires no special training. UICDS is owned by the federal government and available at no-cost. It is built around data standards and the National Information Exchange Model. UICDS enables information sharing across domains, roles, hazards, echelons and applications. UICDS allows information sharing between disparate, proprietary emergency management applications. UICDS users share what, when and with whom they want in accordance with existing or emerging sharing agreements. Users of UICDS are emergency managers and incident commanders in Federal, state, local and tribal organizations as well as critical infrastructure owners/operators. Operational and demonstration pilot programs have been on-going in multiple locations throughout the United States. For more information about UICDS and to download the free software development kit, go to: www.uicds.us.

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/.

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. 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. More information can be found at www.firstresponder.gov.