Office of Infrastructure Protection (IP)

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

IP Training and Education

Threat Detection and Reaction for Retail and Shopping Center Staff This 85-minute session, produced by IP's Office for Bombing Prevention and disseminated by the Commercial Facilities SSA, is modular and utilizes specific foreign and domestic active shooter case studies to present lessons learned and to identify specific considerations for retail and shopping centers. The training discusses signs of criminal and terrorist activity; types of surveillance; and indicators of suspicious behavior. The presentation is available on the DHS HSIN. For access issues contact: CFSTeam@hq.dhs.gov. To access the presentation, please register at: https://connect.hsin.gov/attrrso/event/registration.html.

Active Threat Recognition for Retail Staff A 20-minute session, produced by IP's Office for Bombing Prevention and disseminated by the Commercial Facilities Sector. This is an awareness level Course intended for the 'front-line' retail employee. The training discusses signs of criminal and terrorist activity; types of surveillance; suspicious behavioral indicators; and the Recognition, Reporting, and Reaction considerations in the event of an active shooter incident. The Course is available on the DHS Homeland Security Information Network (HSIN). Access does not require a HSIN account. To access the presentation, please register at: https://connect.hsin.gov/p57147491/ For access issues contact: CFSTeam@hq.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 on ACAMS training, please contact: Traininghelp@hq.dhs.gov

Bombing Prevention Workshop This one-day Workshop, intended for regional level public and private stakeholders and planners from emergency management, security, and law enforcement, enhances the effectiveness in managing a bombing incident. This Workshop reviews the current development of strategies and brings together best practices from regions across multiple localities, disciplines and levels of government. The guided scenario discussion establishes the foundation for the stakeholders within the region to implement a Bombing Prevention Plan. This Workshop can accommodate up to 50 participants. To request training contact your State Homeland Security Advisor.

Chemical Sector Explosive Threat Awareness Training Program The Chemical Sector-Specific Agency (SSA) is offering a series of one day vehicle borne improvised explosive device (VBIED) training sessions to chemical facility security officers. Upon completion, a certificate is awarded to the participant. This course was offered in six locations in FY10 (Dallas, Orlando, New Orleans, St. Louis, Seattle, and Buffalo). For a list of scheduled trainings for FY11, contact the Chemical SSA at ChemicalSector@dhs.gov.

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

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

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

DHS/Commercial Facilities Training Resources Guide pamphlet was developed to promote classroom and independent study programs for DHS partners and private sector stakeholders that build functional skills for disaster

response effectiveness. Subject matter includes cybersecurity, weapons of mass destruction, and natural disaster planning. Available on request, contact the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

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

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

DHS Webinar "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 featured a moderated roundtable discussion of five diverse examples of surveillance and detection. After each scenario, the moderator discussed attendee questions and poll results with a panel of subject matter experts. The panelists discussed what was presented, why it was considered a suspicious activity or behavior, and how to report it. The Webinar also provided information about the resources available for timely reporting of suspicious activities and behaviors. The live Webinar was recorded and is available for download on Homeland Security Information Network-Critical Sectors (HSIN-CS). For more information, please contact CIPAC@dhs.gov.

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

Improvised Explosive Device (IED) Awareness / Bomb Threat Management Workshop This four-hour Workshop enhances and strengthens the participant's knowledge, skills, and abilities in relation to the threat of IEDs. The information presented outlines specific practices associated with Bomb Threat Management including IED awareness, explosive incidents, and bombing prevention. This Workshop is designed to provide one four-hour session that can accommodate up to 50 participants. To request training contact your State Homeland Security Advisor.

Improvised Explosive Device (IED) Search Procedures Workshop This 8-hour Workshop, consisting of lecture and practical exercises, is designed for security personnel and facility managers of sites hosting any event that requires increased IED security preparedness. The information provided during the Workshop focuses on general safeties used for specialized explosives searches and sweeps, and can be tailored to meet the requirements for supporting any event. The Workshop can accommodate 25 participants. To request training contact your State Homeland Security Advisor.

IED Threat Awareness and Response is a 20-minute multi-media module developed by IP's Office for Bombing Prevention that focuses on identifying the threat associated with the Improvised Explosive Device (IED). The training is hosted by the DHS Homeland Security Information Network (HSIN), and while the target audience is Sports Leagues and Public Venues, much of the material is consistent with general IED Awareness. The module objectives relate to the recognition of IEDs, reporting, and response considerations, and is available via URL: https://connect.hsin.gov/e26726633/event/registration.html Additional information can be obtained through the Commercial Facilities Sector-Specific Agency at CFSTeam@hq.dhs.gov

Independent Study Course IS-821 "Critical Infrastructure and Key Resources (CIKR) Support Annex" provides an introduction to the CIKR Support Annex to the National Response Framework. See http://training.fema.gov/emiweb/is/is821.asp, for more information, contact IP_Education@hq.dhs.gov.

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

Independent Study Course IS-871: Dams Sector: Security Awareness (FOUO) is web-based training focused on information provided within the Dams Sector Security Awareness Handbook (FOUO). See http://training.fema.gov/EMIWeb/IS/IS871.asp. For more information, contact the Dams Sector-Specific Agency, dams@dhs.gov.

Independent Study Course IS-872 Dams Sector: Protective Measures (FOUO) is web-based training focused on information provided within the Dams Sector Protective Measures Handbook (FOUO). See http://training.fema.gov/EMIWeb/IS/is872.asp. For more information, contact the Dams Sector-Specific Agency, dams@dhs.gov.

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

Infrastructure Information Collection System (IICS) is a secure, web-based application designed to provide infrastructure protection mission owners with the ability to easily access, search, retrieve, visualize, analyze, and export infrastructure data originating from multiple

disparate sources through a single interface. The IICS enables access to infrastructure-related data that is owned and managed by IP through the Infrastructure Data Warehouse (IDW), as well as infrastructure-related data from various other Federal, State, and local infrastructure protection mission partners. By enabling data from multiple sources and contained within multiple databases to be linked and accessed through one location, the IICS eliminates the need for information to be housed and managed within a single database or by a single entity. Through the IICS, existing infrastructure information awareness and sharing is improved, and it facilitates data maintenance and verification by numerous homeland security partners. For more information, contact IICD-IICS@hq.dhs.gov.

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

IP Sector-Specific Tabletop Exercise Program (IP-SSTEP) Chemical Sector Tabletop Exercise (TTX) is an unclassified and adaptable exercise developed for the purpose of creating an opportunity for public and private Critical Infrastructure and Key Resources (CIKR) stakeholders and their public safety partners to address gaps, threats, issues, and concerns identified in previous exercises and their after-action processes affecting the Chemical Sector. The exercise allows 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 their facility. It also contains everything needed to conduct a Homeland Security Exercise and Evaluation Program (HSEEP) compliant TTX. To obtain a copy of the exercise, contact ChemicalSector@dhs.gov.

Private Sector Counterterrorism Awareness Workshop This one-day Workshop improves the knowledge of private sector security professionals by providing exposure to key elements of soft target awareness, surveillance detection, and improvised explosive device (IED) recognition. The Workshop's training materials enhance and reinforce participants' knowledge, skills, and abilities related to preventing, protecting against, responding to, and recovering from terrorist threats and incidents. The Workshop outlines specific counterterrorism awareness and prevention actions that reduce vulnerability and mitigate the risk of domestic terrorist attacks. This Workshop can accommodate 100 to 250 participants. To request training contact your State Homeland Security Advisor.

Protective Measures Course This two-day Course enhances Commercial Facilities Sector awareness on how to devalue, detect, deter, and defend facilities from terrorism, by providing the knowledge and skills necessary in understanding common vulnerabilities and employing effective protective measures. The Course includes lessons learned and industry best practices in mitigating terrorist attacks. It serves as a follow-up to the Soft Target Awareness Course (description below), focusing more on implementation than awareness. This course can accommodate 35 participants. To request training contact your State Homeland Security Advisor.

Protected Critical Infrastructure Information (PCII) Web-base Training is required for all individuals who wish to access PCII. The PCII Authorized User training provides individuals with an understanding of the background, purpose, and benefits of the PCII program, in addition to safeguarding and handling requirements for PCII. For more information on PCII Authorized User training, please contact: Traininghelp@hq.dhs.gov

Protected Critical Infrastructure Information (PCII) Officer Training provides training on the roles and responsibilities for those with PCII oversight duties within their entity, in addition to a review of PCII Program basics and key messaging training. This training is specifically for those who will be PCII Officers, Deputies, Assistants, and Designees. For more information on PCII Officer training, please contact: Traininghelp@hq.dhs.gov

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

Surveillance Detection Training for Critical Infrastructure and Key Resource Operators and Security Staff This three-day Course explains how protective measures can be applied to detect and deter potential threats to critical infrastructure, as well as the fundamentals for detecting surveillance activity. The Course is designed for commercial infrastructure operators and security staff of nationally significant critical infrastructure facilities. This Course can accommodate 25 participants. To request training contact your State Homeland Security Advisor.

Surveillance Detection Training for Municipal Officials, State and Local Law Enforcement Course This three-day Course provides the knowledge and skills necessary to establish surveillance detection operations to protect critical infrastructure, during periods of elevated threat. Comprised of five modules of informal lecture and two exercises, it provides participants with an awareness of terrorist tactics and attack history and illustrates the means and methods to detect surveillance through practical surveillance detection exercises. This Surveillance Detection Course is designed for municipal security officials and State and local law enforcement with jurisdictional authority over nationally significant critical infrastructure facilities. This Course can accommodate 25 participants. To request training contact your State Homeland Security Advisor.

Threat Detection and Reaction for Retail and 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. To access the 20-minute presentation, visit: https://connect.hsin.gov/p21849699/.

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

IP Guidance Documents/Publications

Active Shooter - How To Respond is a desk reference guide, a reference poster, and a pocket-size reference card to address how employees, managers, training staff, and human resources personnel can mitigate the risk of and appropriately react in the event of an active shooter situation. See http://www.dhs.gov/cfsector. For more information, contact the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

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

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

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

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

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

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

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

Chemical-Terrorism Vulnerability Information (CVI) is the information protection regime authorized by Section 550 of Public Law 109-295 to protect, from inappropriate public disclosure, any information developed or submitted pursuant to Section 550. This includes information that is developed and/or submitted to DHS pursuant to the Chemical Facility Anti-Terrorism Standards (CFATS) regulation which implements Section 550. See www.dhs.gov/chemicalsecurity. For more information, contact the CFATS Help Desk at csat@dhs.gov, (866) 323-2957.

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

more information on Dam and Levee safety please contact the Dams Sector-Specific Agency at dams@dhs.gov.

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

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

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

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

Employee Awareness Video – "No Reservations: Suspicious Behavior in Hotels" is a multi-media training video developed by the Commercial Facilities Sector. The video is aimed at retail employees of lodging venues, alerting them to the signs of suspicious behavior in the workplace that might lead to a catastrophic act. The video is intended to highlight suspicious behaviors and encourage staff to take action when suspicious behavior is identified. This video was distributed to lodging facilities across the nation to promote security awareness. To view or download, please visit: http://www.dhs.gov/criticalinfrastructure. For more information, contact the Commercial Facilities Sector-Specific Agency at CFSTeam@hq.dhs.gov.

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

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

Hotel Security Poster: DHS Hotel and Lodging Advisory The DHS private sector advisory provides hotel employees with an increased awareness of their property's potential to be used for illicit purposes, suspicious behavior and items, and the appropriate actions to take if they notice suspicious activity. This "back of the house" poster is available in both English and Spanish. To obtain copies of the DHS Hotel & Lodging Advisory poster please contact the Commercial Facilities Sector-Specific Agency at CFSTeam@hq.dhs.gov. To download, please visit: www.dhs.gov/cfsector.

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

Infrastructure Protection Report Series (IPRS) is a comprehensive series of For Official Use Only (FOUO) reports containing detailed information for all 18 Critical Infrastructure and Key Resources (CIKR) Sectors focusing on infrastructure characteristics and common vulnerabilities, potential indicators of terrorist activity, potential threats, and associated protective measures. The IPRS is available to vetted private sector critical infrastructure owners and operators with a demonstrated need to know through the Homeland Security Information Network-Critical Sectors (HSIN-CS) (https://cs.hsin.gov/) online secure portal. For more information on the IPRS, private sector CIKR owners and operators should contact DHS Office of Infrastructure Protection Vulnerability Assessments Branch at IPassessments@dhs.gov or the DHS Protective Security Advisor (PSA) Field Operations Staff: PSAFieldOperationsStaff@hq.dhs.gov or (703) 563-3430.

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

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

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

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

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

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

Protective Measures Guide for the U.S. Lodging Industry was 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 For Official Use Only (FOUO) 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, contact the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

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

The Roadmap to Secure Control Systems in the Chemical Sector describes a plan for voluntarily improving cybersecurity in the Chemical Sector. It brings together

Chemical Sector stakeholders, government agencies, and asset owners and operators with a common set of goals and objectives. To obtain a copy of the roadmap or for more information, contact ChemicalSector@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. To obtain a copy of the guide or for more information, contact ChemicalSector@dhs.gov.

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

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

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

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

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

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

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

IP Programs/Services/Events

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

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

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

material. The objective is to implement security enhancements that minimize impact to the user community. For more information, contact the Nuclear Sector-Specific Agency at nuclearSSA@hq.dhs.gov.

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

Chemical Sector Security Summit is an annual industry benchmark event, co-sponsored by DHS and the Chemical Sector Coordinating Council. The Summit consists of workshops, presentations, and discussions covering current security regulations, industry best-practices, and tools for the Chemical Sector. Summit participants include industry professionals throughout the Chemical Sector, senior DHS officials, Congressional staff, and senior government officials. For information on the 2011 Summit, please visit http://www.dhs.gov/files/programs/gc_1176736485793.shtm or contact the Chemical Sector-Specific Agency at ChemicalSector@dhs.gov.

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

Chemical Sector Monthly Suspicious Activity Calls Employees of chemical companies, associations, and agencies who have a need to know information concerning potential physical and cyber threats and vulnerabilities to chemical infrastructure are eligible to listen in on the briefings. This monthly unclassified suspicious activity call for the Chemical Sector is now combined with the Oil and Natural Gas Suspicious Activity Calls and is scheduled for the fourth Thursday of every month at 11:00AM EDT. Contact the Chemical Sector-Specific Agency at ChemicalSector@dhs.gov.

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

Dams Sector Exercise Series (DSES) The Dams SSA, U.S. Army Corps of Engineers, and Green River Valley public and private stakeholders in Washington State are collaborating with multiple critical infrastructure partners to establish a cooperative effort addressing regional disaster resilience issues. The primary goal of *DSES-10: Green River Valley* is to achieve a greater understanding of the potential impacts associated with significant flooding events, and identify those critical infrastructure interdependencies that influence local and regional disruptions. This project will assist public and private stakeholders in jointly identifying, assessing, and improving recovery strategies and business continuity plans, thus enhancing regional resilience and promoting robust partnerships at the local and regional level. See http://www.dses10.org for additional information.

Enhanced Critical Infrastructure Protection (ECIP) Visits are conducted by Protective Security Advisors (PSAs) in collaboration with Critical Infrastructure and Key Resources (CIKR) owners and operators to assess overall facility security and increase security awareness. ECIP Visits are augmented by the Infrastructure Survey Tool (IST), a web-based tool that provides the ability to collect, process, and analyze ECIP survey data in near real time. Data collected during an ECIP visit is consolidated in the IST and then weighted and valued, which enables DHS to develop ECIP metrics; conduct sector-by-sector and cross-sector vulnerability comparisons; identify security gaps and trends across CIKR sectors and sub-sectors; and establish sector baseline security survey scores. Private sector owners and operators interested in receiving an ECIP Visit should contact the PSA Field Operations Staff PSAFieldOperationsStaff@hq.dhs.gov 703-563-3430.

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

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

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

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

Protective Security Advisor (PSA) Program Established in 2004, the PSA Program provides a locally-based DHS infrastructure security expert as the link between State, local, Tribal, territorial, and private sector organizations and DHS infrastructure protection resources. PSAs assist with ongoing State and local critical infrastructure and key resources (CIKR) security efforts, coordinate vulnerability assessments and training, support incident management, and serve as a vital channel of communication between private sector owners and operators of CIKR assets and DHS. Private sector owners and operators interested in contacting their PSA should contact the DHS Protective Security Advisor (PSA) Field Operations Staff: PSAFieldOperationsStaff@hq.dhs.gov or (703) 563-3430.

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

Regional Resiliency Assessment Program (RRAP) is a cooperative DHS led interagency assessment of specific critical infrastructure and key resources (CIKR) and regional analysis of the surrounding infrastructure, including key interdependencies. The emphasis for the RRAP is infrastructure "clusters," regions, and systems. . The assessment and its final report are protected as Protected Critical Infrastructure Information (PCII). Regions are selected collaboratively by State and DHS Officials. Private sector CIKR owners and operators interested in receiving more information on the RRAP should contact the DHS Protective Security Advisor (PSA) Field Operations Staff: PSAFieldOperationsStaff@hq.dhs.gov or (703) 563-3430.

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

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

Security Seminar & Exercise Series for Chemical Industry Stakeholders is a collaborative effort between the DHS Chemical SSA and industry stakeholders such as State chemical industry councils, State homeland security offices, industry trade associations and State emergency management agencies. The intent of the program is to foster communication between facilities and their local emergency response teams by encouraging representatives to share their insight, knowledge, and experiences during a facilitated tabletop exercise. The exercise is catered 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. For more information, contact the Chemical Sector-Specific Agency at ChemicalSector@dhs.gov.

Site Assistance Visit (SAV) is a facility vulnerability assessment focused on identifying security gaps and providing options to enhance protective measures. The SAV uses analyses of critical assets and current security measures, and scenario-based approaches such as assault planning to identify vulnerabilities and develop mitigation strategies. Following the assessment, DHS provides critical infrastructure and key resources (CIKR) owners and operators with an SAV Report, protected as Protected Critical Infrastructure Information (PCII). The report details the facility information and offers options to increase the ability to detect and prevent terrorist attacks and reduce infrastructure vulnerabilities. Private sector owners and operators should contact the DHS Protective Security Advisor (PSA) Field Operations Staff: PSAFieldOperationsStaff@hq.dhs.gov or (703) 563-3430.

IP Web-Based Resources

Automated Critical Asset Management System (ACAMS) is a secure, Web-based portal designed to help State and local emergency responders, such as infrastructure protection planners, homeland security officials, law enforcement personnel, and emergency managers, collect and organize critical infrastructure and key resource (CIKR) asset data as part of a comprehensive CIKR protection program. ACAMS is managed by the Office of Infrastructure Protection (IP) and continues to be developed in partnership with State and local communities and the State, Local, Tribal, Territorial Government Coordinating Council. ACAMS is provided at no cost for State and local use, providing an integrated approach to collecting, protecting and analyzing CIKR asset data. This data is then protected from public disclosure through the Protected Critical Infrastructure Information (PCII) program. The Federal Emergency Management Agency's National Preparedness Directorate and the National Guard Bureau also support ACAMS training through the CIKR Asset Protection Technical Assistance Program (CAPTAP). See www.dhs.gov/ACAMS. For more information, contact ACAMShelp@hq.dhs.gov or (703) 235-3939.

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

Computer Based Assessment Tool (CBAT) is a cross-platform tool that integrates 360 degree geospherical video, geospatial and aerial imagery of facilities, surrounding areas, routes, and other areas of interest with a wide variety of other facility data, including evacuation plans, vulnerability assessments, standard operating procedures, and schematic/floor plans. By integrating this disparate data, the CBAT provides a comprehensive visual guide of a site that assists facility owners and operators, local law enforcement, and emergency response personnel to prepare for and respond to an incident. This resource is protected at the Protected Critical Infrastructure Information (PCII) and For Official Use Only (FOUO) level and is available to vetted private sector critical infrastructure owners and operators with a demonstrated need to know. For more information, contact the DHS PSA Field Operations Staff: PSAFieldOperationsStaff@hq.dhs.gov or (703) 563-3430.

Critical Infrastructure and Key Resources (CIKR) Resource Center was designed to build awareness and understanding of each sector's scope and efforts to ensure CIKR protection and resiliency. The Center offers a centralized location page to find sector goals, plans, priorities, online training modules, activities and achievements, useful links, and other sector-based and cross sector resources. See http://training.fema.gov/emiweb/is/IS860a/CIKR/index.htm. For more information, contact IP_Education@hq.dhs.gov or call (703) 563-3430.

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

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

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

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 HITRAC data call submissions and identification of infrastructure critical systems for industry owners and operators. See www.foodshield.org. For more information, contact Food.AG@hq.dhs.gov.

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

Homeland Security Information Network-Critical Sectors (HSIN-CS) is the primary information-sharing platform between the Critical Infrastructure sector stakeholders. HSIN-CS enables DHS and critical infrastructure owners and operators to communicate, coordinate, and share sensitive and sector-relevant information to protect their critical assets, systems, functions and networks, at no charge to sector stakeholders. Vetted critical infrastructure private sector owners and operators are eligible to access HSIN-CS. To request access to HSIN-CS, please e-mail CIKRISEAccess@hq.dhs.gov. When requesting access, please indicate the critical infrastructure sector to which your company belongs and include your name, company, official e-mail address, and supervisor's name and phone number.

Integrated Common Analytical Viewer (iCAV) provides a suite of free, Web-based, infrastructure-focused geospatial visualization and analysis tools managed by the DHS Office of Infrastructure Protection. The two primary tools in the iCAV suite are the iCAV Next Generation Web-based visualization and analysis platform and the DHS Earth KML service, both of which provide 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. iCAV Next Generation is also the GIS visualization tool for the *Automated Critical Asset Management System* (ACAMS). See www.dhs.gov/icav. For more information, contact iCAV.info@hq.dhs.gov, or (703) 235-4949.

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

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

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

Voluntary Chemical Assessment Tool (VCAT) is a secure, Web-based application that allows owners and operators to identify their facilities' current risk level using an all-hazards approach and facilitates a cost-benefit analysis by allowing them to select the best combination of physical security countermeasures and mitigation strategies to reduce overall risk. For more information or to gain access to the tool, visit http://www.dhs.gov/files/programs/gc_1260467577301.shtm or contact the Chemical Sector-Specific Agency at ChemicalSector@dhs.gov.