Private Sector Resources Catalog

January 2020

U.S. Department of Homeland Security
Washington, DC 20528

Letter from Assistant Secretary

Homeland Security

January 14, 2020

Dear Private Sector Partner,

The responsibility for securing our homeland is shared broadly across federal, state, local, and tribal governments and with the private sector, including large and small businesses, academia, trade associations, and other non-profits. Natural disasters, foreign and domestic terrorist threats, and a myriad of other hazards over the last few years have only highlighted the need for the government and the private sector to work together to ensure your organizations are secure, prepared for all circumstances, and able to rapidly respond to events.

We at the Department of Homeland Security are committed to supporting you. This second iteration of the Private Sector Resources Catalog provides a compendium of DHS programs and points of contact available to the private sector, across all Homeland Security issue areas and inclusive of all DHS Components, Offices, and Directorates.

We appreciate all that you do to help us secure the Homeland, and we welcome your feedback about the Private Sector Resources Catalog and all other matters at PSOResources@hq.dhs.gov.

Sincerely,

John H. Hill
Assistant Secretary

Table of Contents

Department-wide Resources

Civil Rights and Civil Liberties

Blue Campaign to Combat Human Trafficking is a national public awareness campaign and training program, designed to educate the public, law enforcement, and other industry partners to recognize the indicators of human trafficking and how to report. To report suspected human trafficking to Federal law enforcement, the public may use the ICE Homeland Security Investigations (HSI) 24-hour Tip Line 1-866-DHS-2ICE (1-866-347-2423), or for victim assistance, call the National Human Trafficking Hotline (888-3737-888) to reach a non-governmental organization. Informational human trafficking materials are available in a variety of languages, and include public service announcements, brochures, posters, indicator cards, key tag cards, and industry specific toolkits. For more information, see www.dhs.gov/humantrafficking.

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

Community Engagement Roundtables CRCL leads, or plays a significant role, in regular roundtable meetings among community leaders and federal, state, and local government officials. These roundtables bring together American Arab, Muslim, South Asian, Latino, Middle Eastern, Somali, Sikh, and other communities, with government representatives and all levels of law enforcement. CRCL also conducts roundtables with young/youth leaders of diverse communities. For more information, please contact communityengagement@hq.dhs.gov.

DHS Compliance Assurance Program Office (CAPO) The Compliance Assurance Program Office (CAPO) is responsible for providing compliance support services to all DHS Components and their performers. The CAPO ensures DHS-conducted and sponsored activities are compliant with relevant U.S. regulations and laws, international agreements, DHS policies, and relevant standards and guidance. The CAPO's DHS-wide compliance support and oversight functions include six critical areas: biological and chemical arms control, biosafety, biological select agent and toxins, life sciences dual use research of concern, care and use of animals, and human subjects research. The CAPO may also provide export control training, but performers are responsible for performing their own export control due diligence. For more information, see www.dhs.gov/publication/compliance-assurance-program-office or contact treatycompliance@hq.dhs.gov or stregulatorycompliance@hq.dhs.gov.

CRCL Monthly Newsletter informs the public and communities across the country about Office activities including how to file complaints, ongoing and upcoming projects, and opportunities to offer comments and feedback, etc. Newsletters are distributed via email and posted online at: www.dhs.gov/crcl-newsletter. Please contact crcloutreach@hq.dhs.gov for more information.

Civil Rights and Civil Liberties Training at Fusion Centers CRCL partners with the DHS Privacy Office and the Department of Justice's Bureau of Justice Assistance in the development and delivery of civil rights, civil liberties, and privacy training for personnel at state and major urban area fusion centers. In support of this training mission, CRCL maintains a web portal for single point of access to the wide range of resources and training materials that address civil rights, civil liberties, and privacy. To view the portal, please visit: www.it.ojp.gov/PrivacyLiberty.

Environmental Justice Annual Implementation Report Environmental justice (EJ) describes the commitment of the government to avoid placing disproportionately high and adverse burdens on the human health and environment of minority populations or low-income populations through its policies, programs, or activities. Executive Order 12898, *Federal Actions to Address Environmental Justice in Minority Populations and Low-Income Populations* was established in 1994 and directs federal agencies to make achieving

environmental justice part of their mission. As part of our responsibilities in this E.O. 12898, DHS recently published an Environmental Justice Annual Implementation Report. For more information, see www.dhs.gov/dhs-environmental-justice-strategy

Equal Employment Opportunity (EEO) and Diversity Reports The DHS EEO and Diversity Division prepares and submits a variety of annual progress reports relating to the Department's EEO activities: www.dhs.gov/crcl.

Forced Labor Resources The ICE HSI Forced Labor Program coordinates criminal investigations into allegations of forced labor in imported goods in violation of the Tariff Act of 1930 (Title 19 USC §1307) and the Countering America's Adversaries Through Sanctions Act (22 USC § 9241a). When contacting ICE to report instances of forced labor, please provide as much detailed information and supporting documentation as possible, including a full statement of the reasons for the belief that the product was produced by forced labor and that it may be or has been imported into the United States, a detailed description of the product, and all pertinent facts known regarding the production of the product abroad and contact information for the submitter, if possible, for any follow-up questions and discussions. Submissions can be emailed to ice.forcedlabor@ice.dhs.gov.

Guidance to Federal Financial Assistance Recipients Regarding Title VI Prohibition Against National Origin Discrimination Affecting Limited English Proficient Persons CRCL provides guidance for recipients of DHS financial assistance to help them understand and implement their obligations to provide meaningful access for individuals with limited English proficiency (LEP): www.dhs.gov/guidance-published-help-department-supported-organizations-provide-meaningful-access-people-limited.

Human Rights and Vulnerable Populations The CRCL Officer is the designated DHS single point of contact for international human rights treaty reporting and coordination. CRCL works with DHS Components to develop and advance protective policies, procedures, and training for victims of torture and persecution, battered immigrants, trafficked persons, and others needing special attention. For more information, please contact crcl@hq.dhs.gov.

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

"If You Have the Right to Work, Don't Let Anyone Take it Away" Poster is a poster with Department of Justice information regarding discrimination in the workplace. See www.justice.gov/crt/case-document/file/1133936/download.

Introduction to Arab American and Muslim American Cultures is an hour-long training DVD that provides insights from four national and international experts. The training assists law enforcement officers and other personnel who interact with Arab and Muslim Americans, as well as individuals from Arab or Muslim communities. For more information, contact crcl@hq.dhs.gov or visit www.dhs.gov/crcl.

Language Access CRCL leads the Department's efforts to provide meaningful access for LEP individuals. CRCL **also** provides resources, guidance, and technical assistance to recipients of DHS financial assistance. For more information, visit www.dhs.gov/language-access or contact crcl@hq.dhs.gov.

Minority Serving Institutions (MSI) Programs include the Scientific Leadership Awards (SLA) grant program, the Summer Research Team internship program, and a partnership with the Minority Serving Institution Research and Development Consortium (MSRDC). MSI programs improve the capabilities of MSIs to conduct research, education, and training in areas critical to homeland security while building a diverse, highly skilled, technical workforce capable of advancing homeland security goals. The SLA program provides three to five years of institutional support for research and the education advancement of students and early career faculty. The Summer Research Team (SRT) program provides a 10-week, full-time collaborative research experience between recipient MSIs and the DHS Centers of

Excellence. Successful teams can receive additional funding to continue research at the recipient MSI upon completion of the SRT program. The partnership with the MSRDC provides direct funding to MSIs for DHS research and rapid development opportunities. For more information, please visit: Historical Funding Opportunity Announcements http://grants.gov/; Summer Research Team Program www.orau.gov/dhsfaculty/; DHS research projects with MSRDC msrdconsortium.org. For more information, please contact universityprograms@hq.dhs.gov.

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

Online Resources to Prevent Child Exploitation The ICE HSI Child Exploitation Investigations Unit maintains a close working relationship with the National Center for Missing & Exploited Children (NCMEC) in the fight against child exploitation. ICE HSI has a fulltime liaison with the center, and the unit helps disseminate information the center receives via its CyberTipline to more than 50 countries across the globe. Investigations of child sexual exploitation are among HSI's primary investigative priorities.

Project iGuardian provides children, teens, parents, and teachers with information regarding the potential dangers of online environments and how using safe habits online can help prevent many instances of child exploitation. That is why ICE HSI has partnered with the NCMEC's NetSmartz and the Internet Crimes Against Children (ICAC) Task Forces to develop Project iGuardian. For more information, see www.ice.gov/cyber-crimes/resources.

Posters on Common Muslim American Head Coverings, Common Sikh American Head Coverings, and the Sikh Kirpan These training posters provide guidance to Department personnel on ways in which to screen, if needed, Muslim or Sikh individuals wearing various types of religious head coverings; and Sikh individuals carrying a Kirpan (ceremonial religious dagger). These posters are available online at: www.dhs.gov/civil-rights-and-civil-liberties-institute.

Preventing International Non-Custodial Parental Child Abduction DHS partners with the Department of State's Office of Children's Issues to prevent the international abduction of children involved in custody disputes or otherwise against the published order of the court. If you are interested in learning about restricting the international travel of your child, please contact the DOS Office of Children's Issues at preventabduction1@state.gov or the 24 hour hotline 888-407-4747.

Quarterly NGO Civil Rights / Civil Liberties Committee Meeting CRCL hosts regular meetings with representatives of more than 20 civil society organizations primarily working on matters at the intersection of immigration and civil and human rights. Assisted by extensive grassroots networks, committee members articulate the concerns of organizations and communities across the country on these issues. The CRCL Officer meets quarterly with the committee to discuss CRCL's activities, and respond to NGO concerns related to DHS policies, programs, and activities. For more information, please contact crcl@hq.dhs.gov.

Resources for Victims of Human Trafficking and Other Crimes USCIS offers resources for victims of human trafficking and certain other crimes and the organizations that serve them. For information about obtaining T or U nonimmigrant status, please see www.uscis.gov/tools/humanitarian-benefits-based-resources/resources-victims-human-trafficking-other-crimes.

Stop the Bleed is a national awareness campaign and call-to-action to cultivate grassroots efforts that encourage bystanders to become trained, equipped, and empowered to help in a bleeding emergency before professional help arrives. To learn more, see www.dhs.gov/stopthebleed.

Victim Assistance Program (VAP) provides information and assistance to victims of federal crimes, including human trafficking, child exploitation, human rights abuse, and white collar crime. VAP headquarters personnel, as well as Victim Assistance Specialists (VAS) and Victim Assistance Coordinators (VAC) in the field, also provide training and technical assistance to special agents, law enforcement partners, and other agencies. Full-time Forensic Interview

Specialists are also available to conduct developmentally appropriate, legally defensible, and victim-sensitive interviews in HSI cases involving child, adolescent, or special needs victims. VAP has developed informational brochures on human trafficking victim assistance, crime victims' rights, white collar crime, and the victim notification program. For more information, please contact VAP at victimassistance.ice@dhs.gov or 866-872-4973.

Victim of Immigration Crime Engagement (VOICE) Office was established to acknowledge and provide information to crime victims and their families who have been impacted by crimes committed by individuals with a nexus to immigration. VOICE can help victims of crime, witnesses of crimes, individuals with a legal responsibility to act on behalf of a victim or witness (e.g., attorneys, parents, legal guardians), and individuals acting at the request of a victim or witness. Victims can sign up to receive automated custody status information about an alien in custody through the Department of Homeland Security Victim Information and Notification Exchange (DHS-VINE), releasable criminal or immigration history about an alien, or access to social service professionals available to refer victims to local service providers. ICE has established a toll-free hotline staffed with operators who will take calls to ensure victims receive the support they need. The number is 1-855-48-VOICE or 1-855-488-6423 (Mon.-Fri. 8am-8pm EST).

Economic Analysis

DHS Center of Excellence: Center for Accelerating Operational Efficiency (CAOE) led by Arizona State University, develops and applies advanced analytical tools and technologies to enhance planning, information sharing and real-time decision-making in homeland security operations. For more information, see https://caoe.asu.edu or contact universityprograms@hq.dhs.gov.

DHS Emeritus Center of Excellence: The National Center for Risk and Economic Analysis of Terrorism Events (CREATE) developed a suite of tools for security patrol scheduling using applied game theory. Assistant for Randomized Monitoring Over Routes(ARMOR) tools generate intelligently randomized patrol schedules that optimize countermeasures' effectiveness and deterrence effect. ARMOR software randomizes patrols, inspections, schedules, plans or actions carried out by security agencies. ARMOR has been in use at Los Angeles Airport (LAX) to randomize security checkpoints and canine patrols since 2007. Variants of ARMOR have been adopted by the U.S. Federal Air Marshals Service, Transportation Security Agency, and U.S. Coast Guard. For more information, see https://create.usc.edu/ or contact universityprograms@hq.dhs.gov.

Outreach and Engagement

Advisory Committee on Commercial Operations of Customs and Border Protection (COAC) The Advisory Committee on Commercial Operations of Customs and Border Protection (COAC) advises the Secretaries of the Department of the Treasury and the Department of Homeland Security on the commercial operations of U.S. Customs and Border Protection and related DHS functions. For more information, see www.cbp.gov/trade/stakeholder-engagement/coac.

The Border Interagency Executive Council (BIEC) The Border Interagency Executive Council (BIEC) is an interagency working group formally established by Executive Order 13659. The BIEC serves as an Executive Advisory Board charged with assisting federal agencies in their efforts to enhance coordination across customs, transport security, health and safety, sanitary, conservation, trade, and phytosanitary agencies with border management authorities and responsibilities to measurably improve supply chain processes and the identification of illicit and non-compliant shipments. BIEC membership includes senior leadership from Departments and agencies with border management authorities and responsibilities, as well as representatives from the Executive Office of the President. Per Executive Order 13659, the BIEC is to measurably improve supply chain processes and the identification of illicit and non-compliant shipments. For more information, visit www.cbp.gov/trade/trade-community/border-interagency-executive-council-biec/biec-frequently-asked-questions-faqs.

CBP Industry Partnership and Outreach Program serves as CBP's primary interface to industry for education and information on procurement opportunities, and it's Small Business Program. The program is responsible for processing unsolicited proposals and includes in its organizational structure, CBP's

procurement ombudsman. Officially serving as CBP's "Task and Delivery Order Ombudsman," the program director addresses vendors' concerns or complaints, relating to task or delivery order award procedures. All inquiries are handled in an impartial (and upon request, confidential) manner. Vendors seeking information on how to do business with CBP should go to www.cbp.gov/xp/cgov/toolbox/contacts/contracting/

U.S. Customs and Border Protection (CBP) Intergovernmental Public Liaison A component of the CBP Commissioner's Office, Intergovernmental Public Liaison (IPL) Office strives to build and maintain effective relationships with state, local, tribal, and territorial governments through regular, transparent and proactive communication. Governmental questions regarding issues and policy pertaining to countering terrorism and transnational crime, border security, and trade and travel facilitation can be referred to the IPL at: cbp-intergovernmental-public-liaison@cbp.dhs.gov or 202-325-0775.

Customs and Border Protection User Fee Advisory Committee (UFAC)
The UFAC advises the Secretary of the Department of Homeland Security (DHS) on issues related to the performance of inspections coinciding with the assessment of an agriculture, customs, or immigration user fee. This guidance should include, but is not limited to, the time period during which such services should be performed, the proper number and deployment of inspection officers, the level of fees, and the appropriateness of any proposed fee.
www.cbp.gov/trade/stakeholder-engagement/user-fee-advisory-committee

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

CWMD Industry Engagement Program
The DHS Countering Weapons of Mass Destruction Office (CWMD) works to counter attempts by terrorists and other threat actors to carry out an attack against the United States or its interests using a weapon of mass destruction. To accomplish this mission, CWMD works with industry partners to:

- develop and acquire technology;
- invest in basic and applied research to support new technologies;
- improve the performance of deployed technologies; and
- strengthen the nation's bio-detection programs.

For more information, please contact cwmd.iep@hq.dhs.gov.

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

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

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

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

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

FEMA Industry Liaison Program establishes strategic relationships with suppliers and stakeholders; serves as an information provider for suppliers seeking to do business with FEMA; and connects suppliers with program offices in support of FEMA's mission. Vendors seeking to do business with FEMA in support of a disaster recovery effort, please be aware that in accordance with the Robert T. Stafford Act (specifically section 307), FEMA's goal is to seek local companies within the disaster area for goods and services related to a specific disaster when practical and feasible. Visit www.fema.gov/industry-liaison-program.

Emergency Support Function (ESF) #14 – Cross-Sector Business and Infrastructure supports the coordination of cross-sector operations, including stabilization of key supply chains and community lifelines, among infrastructure owners and operators, businesses, and their government partners. ESF #14 is complementary to the Sector-Specific Agencies (SSA) and other ESFs and is a mechanism for entities that are not aligned to an ESF or have other means of coordination. ESF #14 supports growing efforts to enable assistance among critical infrastructure sectors and helps coordinate and sequence such operations to mitigate cascading failures between them. ESF #14 also integrates SSA incident response operations with ESFs and other relevant public-private sector coordinating entities. The Federal Government seeks to enable—where possible—business and infrastructure owners and operators that have the authorities, capabilities, and resources to stabilize community lifelines. For more information, visit www.fema.gov/media-library/assets/documents/25512.

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

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

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

Hometown Security Initiative works to protect against attacks on public gatherings and public places to enhance the Nation's security. DHS engages closely with our private sector and community partners to provide advice and assistance about protective measures they may implement to protect facilities and venues. DHS provides tools and resources to our communities because the Department recognizes that communities are the first line of defense in keeping the public safe and

secure. "Connect – Plan – Train – Report" is a simple four-step action plan for small and medium sized businesses, non-profits, and faith-based organizations to consider when thinking about the safety and security of their businesses, members and customers. To learn more about the Hometown Security Initiative, please visit www.dhs.gov/cisa/hometown-security.

ICE Office of Public Affairs (OPA) is dedicated to building understanding and support for the agency mission through outreach to employees, the media and the general public. ICE field public affairs officers are stationed throughout the country and are responsible for regional media relations in specific geographic areas. For more information, see www.ice.gov or contact publicaffairs.iceofficeof@dhs.gov, or 202-732-4646.

ICE Office of Partnership and Engagement (OPE) coordinates outreach efforts with the public, key stakeholders, and ICE leadership to increase local and national awareness of U.S. Immigration and Customs Enforcement's (ICE) mission, while building relationships and fostering trust in our communities. OPE, headquartered in Washington, D.C. has two distinct offices: the Community Engagement Office and the Victims Of Immigration Crime Engagement (VOICE) Office. The Community Engagement Office has a cadre of 25 community relations officers (CROs) in field offices across the United States who serve as liaisons to the public, key stakeholders, and ICE leadership. CROs are co-located throughout the country at either the Special Agent in Charge (SAC) or Field Office Director (FOD) field offices. The VOICE Office assists victims impacted by crimes committed by individuals with a nexus to immigration. For more information, see www.ice.gov/leadership/ope, or contact the Community Relations Officer in your area, www.ice.gov/contact/ope.

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

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

FEMA Office of External Affairs The FEMA Office of External Affairs (OEA) engages, informs and educates the private sector and other external stakeholders on the Agency's programs and initiatives to achieve FEMA's mission of helping people before, during and after a disaster.

Private Sector Office/FEMA Office of Response and Recovery FEMA established the Private Sector Division (PSD) in 2007 to communicate, cultivate and advocate for collaboration between the U.S. private sector and FEMA, to support FEMA's capabilities and to enhance national preparedness, protection, response, recovery, and mitigation of all hazards. PSD operates the National Business Emergency Operations Center. Contact: Fema-private-sector@dhs.gov

Regional Private Sector Liaisons FEMA designated a private sector liaison in each of its 10 regions to cultivate two-way communication between FEMA, state/local/tribal/territorial officials, and the private sector during steady state and disaster operations. For more information, please contact fema-private-sector-communications@fema.dhs.gov.

Science and Technology Directorate (S&T) Industry Liaison: Industry Liaison serves as S&T's primary interface to the private sector by communicating S&T's requirements and partnership tools. This office is responsible for responding to inquiries and directing partners to the appropriate point of contact; and coordinating S&T's engagement and outreach opportunities with industry. For more information, email sandt.innovation@hq.dhs.gov.

Cybersecurity and Infrastructure Security Agency (CISA) CISA is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future. CISA's partners in this mission

span the public and private sectors. CISA's comprehensive understanding of the risk environment and the corresponding needs identified by its stakeholders drives programs and services provided. CISA seeks to help organizations better manage risk and increase resilience using all available resources, whether provided by the Federal Government, commercial vendors, or their own capabilities. For more information visit: www.dhs.gov/cisa.

Policy Guidance

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

Critical Infrastructure Training Portal Housed on the Homeland Security Information Network – Critical Infrastructure (HSIN-CI), this portal offers a single point of entry for relevant training, guidance documents, presentations, brochures, instructional videos, and links to external educational resources. The portal is available to HSIN-CI users only. For more information, see www.dhs.gov/homeland-security-information-network-hsin.

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

IS-1170 Introduction to the Interagency Security Committee (ISC) is the first course in the independent study ISC web-based training series. The purpose of this series of courses is to provide federal facility security professionals, engineers, building owners, construction contractors, architects, and the public with basic information pertaining to the ISC and its facility security standards, processes, and practices. This course provides an overview of the history of the ISC, its mission and organization, and a basic outline of the ISC risk management process. The course can be accessed at: https://training.fema.gov/is/courseoverview.aspx?code=is-1170. For more information, contact independent.study@fema.dhs.gov.

IS-1171: Overview of Interagency Security Committee (ISC) Publications is the second course in the ISC web-based training series. This course provides an overview of ISC facility security standards and policies and other documents that support the Risk Management Process (RMP). The course can be accessed at: https://training.fema.gov/is/crslist.aspx?all=truehttp://training.fema.gov/emiweb/is/is890a.asp. For more information contact isc.dhs.gov@hq.dhs.gov.nstac

Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practices Guide (Non-FOUO) This document streamlines existing ISC policy on active shooter incidents into a cohesive policy and guidance document that agencies housed in federal facilities can use as a reference to enhance preparedness for an active shooter incident. This version is publicly available as a reference document for the private sector to include a wider audience that may benefit from the information presented therein. For more information: www.dhs.gov/publication/isc-planning-and-response-active-shooter-guide

2019 Edition - Violence in the Federal Workplace: A Guide for Prevention and Response This document provides guidance on how agencies can develop a workplace violence program capable of preparing for, preventing, and responding to incidents of workplace violence. The Appendices: address how to evaluate threats; provide example policy, checklists, and a list of other free and online materials; and include several case studies for consideration.

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

National Disaster Recovery Framework (NDRF)
The National Disaster Recovery Framework is a guide that enables effective recovery support to disaster-impacted States, Tribes, Territorial and local jurisdictions. It provides a flexible structure that enables disaster recovery managers to operate in a unified and collaborative manner. It also focuses on how best to restore, redevelop and revitalize the health, social, economic, natural and environmental fabric of the community and build a more resilient Nation. Visit: www.fema.gov/national-disaster-recovery-framework.

National Response Framework (NRF) is a guide for how the nation responds to all types of disasters and emergencies. It is built upon scalable, flexible, and adaptable coordinating structures to align key roles and responsibilities across the nation, linking all levels of government, nongovernmental organizations, and the private sector. It is intended to capture specific authorities and best practices for managing small- or large-scale incidents, terrorist attacks or catastrophic natural disasters. The fourth edition of the NRF focuses on outcomes-based response through the prioritization of the rapid stabilization of community lifelines. The latest edition also emphasizes the importance of enhancing unity of effort between government and private sector through increased coordination and collaboration. For more information, visit www.fema.gov/national-planning-framework.

Cybersecurity and Infrastructure Security Agency (CISA) Sector-Specific Agency Sector Snapshots, Fact Sheets and Brochures These products provide a quick look at CISA sectors and contain sector overviews as well as information on sector partnerships, critical infrastructure protection issues and priority programs. These products include fact sheets and brochures for chemical, commercial facilities, critical manufacturing, dams, emergency services and nuclear sectors. Additional materials are available on request. For more information, contact nipp@dhs.gov.

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

Sector Specific Plans (SSPs) support the National Infrastructure Protection Plan by establishing a coordinated approach to national priorities, goals, and requirements for critical infrastructure protection. Each SSP provides the means through which the NIPP is implemented for each sector, as well as a national framework to address the sector's unique characteristics and risk landscape. DHS collaborates with government and private sector partners to develop, update, and maintain SSPs for the Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Emergency Services, Information Technology, and Nuclear Sectors. For more information, or to review copies of the 2015 SSPs visit www.dhs.gov/files/programs/gc_1179866197607.shtm.

Privacy

The DHS Privacy Office sustains privacy protections and the transparency of government operations while supporting the DHS mission. The DHS Privacy Office ensures DHS programs and operations comply with federal privacy laws and policies. Members of the public can contact the Privacy Office with concerns or complaints regarding their privacy. For more information, visit www.dhs.gov/privacy or contact privacy@hq.dhs.gov, 202-343-1717.

Privacy Impact Assessments (PIAs) are decision-making tools used to identify and mitigate privacy risks at the beginning of and throughout the development life cycle of a

program or system. They help the public understand what personally identifiable information (PII) the Department is collecting, why it is being collected, and how it will be used, shared, accessed, and stored. All PIAs issued by DHS may be found here: www.dhs.gov/files/publications/editorial_0511.shtm.

DHS Privacy Office Disclosure and Transparency Private sector organizations can use the Freedom of Information Act (FOIA) to get specific information from Federal agencies. To view the process for submitting a FOIA request, or to see a library of past requests, please visit www.dhs.gov/xfoia/editorial_0579.shtm or sign up to receive notices regarding new disclosures added to the FOIA Library at www.dhs.gov/subscribe-foia-library-notifications.

DHS Data Privacy and Integrity Advisory Committee (DPIAC) provides advice at the request of the Secretary of Homeland Security and the DHS Chief Privacy Officer on programmatic, policy, operational, administrative, and technological issues within the DHS that relate to personally identifiable information, as well as data integrity and other privacy-related matters. To review DPIAC recommendations and for information on public meetings, please visit www.dhs.gov/privacy-office-dhs-data-privacy-and-integrity-advisory-committee.

DHS Privacy Office Annual Reports to Congress: These reports, which highlight the accomplishments of the Privacy Office, are posted on our website at: www.dhs.gov/privacy.

Protecting Against Fraud & Counterfeiting

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

Commercial Fraud ICE HSI investigates commercial fraud involving imports into and exports from the Unites States. The ICE HSI Commercial Fraud Programs Unit, which is led by the National Intellectual Rights Coordination Center, prioritizes health and safety violations, U.S. economic interests, and duty collection. For more information, see www.iprcenter.gov.file-repository/commercial-fraud-fact-sheet.pdf/view.

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

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

How to Protect Your Rights The flow of counterfeit and pirated goods is a global problem that requires vigorous collaboration between customs agencies and rights owners to ensure effective intellectual property enforcement at the border. Working with CBP provides many benefits for rights owners of

patents, copyrights, and trademarks to ensure maximum intellectual property rights protection. The three steps you can take to maximize your relationship with CBP are e-Recordation, e-Allegations, and information sharing. For more information, visit www.cbp.gov/linkhandler/cgov/trade/priority_trade/ipr/legal/ipr_guide.ctt/ipr_guide.pdf.

HSI Illicit Finance and Proceeds of Crime Unit (IFPCU) recognizes the private sector represents America's first line of defense against money laundering. In furtherance of ICE HSI's mission of safeguarding the citizens and critical infrastructure of the United States from threats posed by the illegal movement of people and goods into and through the U.S., IFPCU partners with the business community, along with state and federal agencies, to combat financial and trade crimes. Through various outreach initiatives, IFPCU works to identify and eliminate vulnerabilities within the U.S. financial, trade, and transportation sectors. These vulnerabilities have the potential to be used by criminal organizations and terrorist groups to finance their illicit activities and avoid detection by law enforcement. In addition to its outreach efforts, IFPCU periodically publishes articles and provides information related to current industry trends and other topics of interest at www.ice.gov/cornerstone.

HSI Trade-based Money Laundering (TBML)/Trade Transparency Unit
The primary mission of ICE HSI's Trade Transparency Unit (TTU) is to aggressively identify and thwart TBML. TTUs conduct analysis of trade data and provide support to financial and trade investigations. ICE HSI works with the public and financial institutions to combat TBML, which entails the use of international trade transactions in an attempt to hide the true source of funds. Combatting TBML is a shared mission between the federal government, the private sector, and foreign partners. Report suspicious activity by contacting your local ICE HSI office or by emailing reporttbml@ice.dhs.gov. For more information, visit www.ice.gov/trade-transparency.

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

ICE HSI's Counter-Proliferation Investigations (CPI) unit, within the agency's Global Trade Investigations Division, safeguards national security by preventing sensitive U.S. technologies and weapons from reaching the hands of adversaries. The CPI unit specifically targets the trafficking or illegal export of: materials used to manufacture weapons of mass destruction, chemical, biological, radiological and nuclear materials, military equipment and technology, controlled dual-use commodities and technology, and firearms and ammunition. To report suspicious activity, call 1-866-DHS-2-ICE (1-866-347-2423) or complete ICE HSI's online tip form at www.ice.gov/tipline.

Intellectual Property Rights (IPR) Fact Sheet
U.S. Customs and Border Protection enforces IPR, most visibly by seizing products that infringe IPR such as trademarks and, copyrights that have been recorded with CBP, or are subject to exclusion orders issued by the U.S. International Trade Commission. The theft of intellectual property and trade in fake goods threaten America's economic vitality and national security, and the American people's health and safety. For more information, please visit www.cbp.gov/trade/priority-issues/ipr

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

Intellectual Property Rights (IPR) Enforcement: A Priority Trade Issue
Counterfeit trade and pirated goods threatens America's innovation economy, the competitiveness of our businesses, the livelihoods of U.S. workers, national security, and the health and safety of consumers. These illegitimate goods are associated with

smuggling and other criminal activities, and often funds criminal enterprises. For more information, visit www.cbp.gov/trade/priority-issues/ipr.

Intellectual Property Rights (IPR) Help Desk can provide information and assistance for a range of IPR related issues including: IPR border enforcement procedures, reporting allegations of IPR infringement, assistance for owners of recorded trademarks and copyrights to develop product identification guides and to assist officers at ports of entry with identifying IPR infringing goods. For more information, contact iprhelpdesk@cbp.dhs.gov.

Intellectual Property Rights (IPR) Seizure Statistics CBP maintains statistics on IPR seizures made by the DHS. See www.cbp.gov/trade/priority-issues/ipr/statistics.

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

Online Detainee Locator System The online system can be used to locate a detainee who is currently in ICE custody. Detainees may be located using alien number (A-number) and country of birth or by biographical information (first name, last name, country of birth and date of birth). For more information, visit https://locator.ice.gov/odls/homepage.do.

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

Operation Guardian is a multi-agency effort to combat the increasing importation of substandard, tainted, and counterfeit products that pose a health and safety risk to consumers. The identification of these commodities has led to the successful detention and seizure of numerous containers of hazardous products. For more information, visit www.iprcenter.gov.ip-theft/ongoing-operations.

Operation In Our Sites specifically targets websites and their operators that distribute counterfeit and pirated items over the Internet, including counterfeit pharmaceuticals and pirated movies, television shows, music, software, electronics, and other merchandise, as well as products that threaten public health and safety. For more information, visit www.iprcenter.gov/file-repository/ipu-operation-in-our-sites-2016.docx/view.

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

U.S. International Trade Commission (USITC) Exclusion Orders CBP also enforces exclusion orders issued by the U.S. International Trade Commission, the majority of which are patent-based. Requests for rulings on the admissibility of redesigned articles or articles that were not adjudicated by the USITC may be sent to iprbranch.itc337.rulings@cbp.dhs.gov.

Intellectual Property Rights (IPR) e-Recordation and IPR Search The first step in obtaining IPR protection by CBP is to record validly registered trademarks and copyrights with CBP through the Intellectual Property Rights e-Recordation (IPRR) online application. Once recorded, trademarks and copyrights can be viewed on Intellectual Property Rights Search (IPRS), the

searchable, public version of CBP's recordation database. Recordation and related inquiries should be directed to http://iprs.cbp.gov/

Gray Market and Lever-Rule Protection
Requests for enhanced trademark recordation status relative to restrictions on gray market articles and articles that are physically and materially different (Lever-Rule) than those authorized for sale in the U.S. may be submitted to iprquestions@cbp.dhs.gov. For more information see 19 CFR 133.23, available at www.ecfr.gov/cgi-bin/text-idx?sid=a67e218dc90d00a19ed0e232c55eac79&mc=true&node=pt19.1.133&rgn=div5#se19.1.133_123.

Research and Product Development

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

Broad Agency Announcements (BAA) are acquisition instruments for research and development projects which address DHS capability gaps or advance technical knowledge in the basic sciences and to gain access to original, state-of-the-art, basic and applied research proposals. DHS S&T uses BAAs in two ways: Long-Range Broad Agency Announcements (LRBAA) and Targeted BAAs. LRBAAs are used for ongoing areas of need that support the DHS overarching mission areas. Targeted BAAs are often used when there is a need that has not been met and there is a programmatic requirement to find and propose a solution within a scheduled timeframe. For submission instructions, evaluation criteria, research topics, and to apply online, visit: https://baa2.st.dhs.gov.

The Catalog of Federal Domestic Assistance (CFDA) provides a full listing of all Federal programs available to state and local governments (including the District of Columbia); federally-recognized Indian tribal governments; Territories (and possessions) of the United States; domestic public, quasi-public, and private profit and non-profit organizations and institutions; specialized groups; and individuals. DHS Programs can be found under the 97.000 series or are searchable through the tools on CFDA's main page. For more information, see www.cfda.gov.

Cooperative Research and Development Agreements (CRADAs) are part of the National Technology Transfer Program, designed to assist federal laboratories in leveraging taxpayer dollars. The DHS CRADA is intended for R&D collaborations with an innovative or entrepreneurial non-Federal entity that can succeed in moving federally funded technology to the commercial market. Technology developed in the federal laboratories can utilize the CRADA program to establish partnerships for research and development in areas with potential to advance homeland security missions. For more information, contact crada@hq.dhs.gov.

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

DHS Silicon Valley Innovation Program (SVIP) expands DHS S&T's reach to find new technologies that strengthen national security with the goal of reshaping how government, entrepreneurs, and industry work together to find cutting edge solutions. The program reaches out to innovation communities across the nation and around the world to harness the commercial R&D ecosystem for technologies with government applications and to co-invest in and accelerate technology transition-to-market. For more information visit www.dhs.gov/science-and-technology/svip.

DHS Technology Transfer and Commercialization Program serves as the centralized point to manage technology transfer activities throughout DHS and the DHS' lab network. This program also promotes the transfer and/or exchange of technology with industry, state and local governments, academia, and other federal agencies. The technologies developed and evaluated within DHS can have potential commercial applications and dramatically enhance the competitiveness of individual small businesses, as well as expanding areas of exploration and cooperation for non-federal partners. For more information, visit www.dhs.gov/xabout/structure/gc_1264538499667.shtm.

DHS Small Business Innovation Research (SBIR) Program is designed to stimulate technological innovation; strengthen the role of small business in meeting DHS research and development needs; foster and encourage participation of socially and economically disadvantaged persons and women-owned small business concerns in technological innovation; and increase the commercial application of DHS-supported research or research and development results. SBIR research areas are chosen for their applicability to support homeland security missions and address the needs of the eight DHS operational units. Additional information can be found at https://sbir2.st.dhs.gov.

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

The Homeland Security Science and Technology Advisory Committee (HSSTAC) provides consensus scientific and technical advice to the Under Secretary for Science and Technology. Its members include representatives of the private sector. Its activities focus on strengthening America's security and resiliency by providing knowledge products and innovative technology solutions for the Homeland Security Enterprise. Among its tasks, the committee advises the Under Secretary on how best to leverage related technologies funded by the private sector. For more information, see www.dhs.gov/homeland-security-science-and-technology-advisory-committee-hsstac.

Israel-U.S. Binational Industrial Research and Development (BIRD) Foundation, in partnership with the DHS Science and Technology Directorate, is designed to stimulate, promote and support joint (non-defense) industrial R&D of mutual benefit to Israel and the United States. Established under the agreement between the Government of the United States of America and the Government of the State of Israel on Cooperation in Science and Technology for Homeland Security Matters, BIRD Homeland Security funds R&D cooperation between two companies or a company and a university / research institution (one from the U.S. and one from Israel) to foster and support joint development for advanced technologies in the homeland security mission. For information on current and future solicitations, research topics, submission instructions, evaluation criteria, and how to apply, visit: www.birdf.com/.

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

National Urban Security Technology Laboratory (NUSTL) provides the nation's first responder community with services, products and tools to prevent, protect against, mitigate, respond to and recover from homeland security threats and events. NUSTL conducts testing and evaluation (T&E) that influences technology development and informs acquisition and deployment decisions. NUSTL leads operational T&E and field assessments; performs independent laboratory testing; conducts technology performance characterization; and holds operational experimentations with end users and private industry manufacturers. NUSTL

also manages a radiological/nuclear response and recovery research and development portfolio which provides technical support, tools and guidance in advance of a radiological/nuclear incident to allow for state and local agencies to initiate a response in the first minutes and hours. NUSTL's actionable guidance and technology solutions enhance response capabilities for:

- Managing the complexity of a radiological response;
- Incident characterization and initial decision-making;
- Immediate lifesaving and issuing of protective actions;
- Stabilization and control of impacted areas; and
- Site cleanup and decontamination.

NUSTL's broad ranging relationships with the homeland security community enable the use of the New York metropolitan area as an urban test bed for the diverse technologies and systems being developed to prepare and protect our nation. For more information, contact nustl@hq.dhs.gov.

Planning Guidelines and Design Standards (PGDS) for Checked Baggage Inspection Systems incorporate insights and experience of industry stakeholders, including airport and airline representatives, planners, architects, baggage handling system designers, and equipment manufacturers. The PGDS assists planners and designers in developing cost-effective solutions and to convey TSA requirements for checked baggage inspection systems. The PGDS emphasizes best practices associated with screening system layouts and addresses other factors necessary to actively manage system costs and performance. For more information, see www.tsa.gov/press/releases/2009/12/07/updated-planning-guidelines-and-design-standards-checked-baggage or contact the TSA Contact Center, 866-289-9673.

Prize Challenges provide incentives that inspire and mobilize a diverse set of non-traditional talent to address a wide range of homeland security challenges. This program seeks to find solutions to the challenges faced by DHS leveraging crowdsourcing by removing typical barriers for partnering with the federal government. For more information about current and past DHS Prize Challenges visit: www.dhs.gov/science-and-technology/prize-competitions.

Project 25 Compliance Assessment Program (P25 CAP) was established, in coordination with the National Institute of Standards and Technology (NIST), to provide a process for ensuring that equipment complies with P25 standards, meets performance requirements, and is capable of interoperating across manufacturers. P25 CAP allows emergency responders to confidently purchase and use P25-compliant products. For more information, see www.dhs.gov/science-and-technology/p25-cap or contact p25cap@dhs.gov.

Research and Standards Integration Program (RSI) interfaces with public and private sector organizations to advance the future state of cybersecurity and communications through Research and Development (R&D) and standards. RSI seeks input from researchers to determine if their R&D projects map to Cybersecurity and Communications (CS&C) R&D requirements, particularly to identify relevant federally funded research. For more information, contact rsi@hq.dhs.gov.

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

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

Support Anti-Terrorism by Fostering Effective Technologies Act (SAFETY Act) evaluates and qualifies technologies for liability protection in accordance with the SAFETY Act of 2002 and the supporting regulations of the Final Rule (6

CFR Part 25) implemented on July 10, 2006. The SAFETY Act provides risk management and liability protections for sellers of Qualified Anti-Terrorism Technologies. The purpose of the SAFETY Act is to ensure that the threat of liability does not deter potential manufacturers or sellers of effective anti-terrorism technologies from developing, deploying and commercializing these technologies that meet homeland security objectives. For more information, see www.safetyact.gov or contact safetyacthelpdesk@dhs.gov, 866-788-9318.

Best Practices for Anti – Terrorism Security (BPATS). DHS has national leadership responsibilities for managing risks involving critical infrastructure, key resources and events. DHS has identified commercial facilities as key assets in the critical infrastructure/key resource sector and encourages the widespread deployment of effective anti-terrorism technologies, services and capabilities. Building security programs may receive designation under the SAFTEY Act. DHS S&T worked in partnership with the National Institute for Building Sciences to help building owners and managers identify a set of best operational security practices for metropolitan commercial office buildings, referred to as Best Practices for Anti-Terrorism Security (BPATS) and a corresponding web-based methodology for performing security assessments on commercial buildings. BPATS allows building owners to evaluate their operations end-to-end and identify the steps needed to address the risk assessment before applying for SAFETY Act protections. For more information, visit www.safetyact.gov or https://bpatsassessmenttool.nibs.org.

System Assessment and Validation for Emergency Responders (SAVER) Program, managed by the DHS National Urban Security Technology Laboratory (NUSTL), assists responders making procurement decisions by conducting objective operational assessments and technical verifications of commercially available responder equipment. SAVER provides those results, along with other relevant equipment information, to the responder community in an operationally useful form. SAVER provides information that enables decision-makers and responders to better select, procure, use, and maintain emergency responder equipment. More information and copies of SAVER reports can be obtained at www.dhs.gov/science-and-technology/saver or by e-mail at nustl@hq.dhs.gov.

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

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

Social Media Engagement

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

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

CRCL's Facebook Page allows our Office to connect with the public and diverse communities across the country. We share information about our work to integrate civil rights and civil liberties into DHS programs, policies, strategies and activities. We engage with our followers to receive feedback and learn about issues occurring in communities across the country. Follow us at: www.facebook.com/civilrightsandcivilliberties

Customs and Border Protection (CBP) Social Media tools provides information to engage with and inform the public about CBP programs and current activities. Social Media tools include: CBP Twitter channel; www.twitter.com/cbp; a Flickr account that features CBP photo stream at www.flickr.com/photos/54593278@n03/; and a YouTube channel for hosting video content at www.youtube.com/user/customsborderprotect.

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

FEMA App Download the FEMA App to locate and get directions to open shelters across the state and receive weather alerts from the National Weather Service for up to five different locations anywhere in the United States.

FEMA Podcast An audio series available to anyone interested in learning more about the agency, hearing about innovation in the field of emergency management, and listening to stories about communities and individuals recovering after disasters. The FEMA Podcast is available on Apple iTunes and Google Play to stream or download. The podcast is approximately 20 to 30 minutes in length and new episodes will be offered every two weeks. Also included in the weekly podcast is a link to the transcript. Visit www.fema.gov/podcast.

FEMA Private Sector Communicators Collaboration The FEMA Office of External Affairs provides a platform for public and private sector communicators to coordinate and synchronize messaging priorities and communications plans during disasters. For more information, contact fema-private-sector-communications@fema.dhs.gov.

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

Follow FEMA online at www.fema.gov/blog, www.twitter.com/fema, www.twitter.com/femaespanol, www.facebook.com/fema, www.facebook.com/femaespanol, and www.youtube.com/fema. Also, follow Acting Administrator Pete Gaynor's activities @fema_pete.

ICE Social Media channels provide important news and information about the agency's mission, policies and operations. Follow ICE on Facebook at www.facebook.com/wwwice.gov; on Twitter at www.twitter.com/icegov; on YouTube at www.youtube.com/user/wwwicegov; and on Instagram at www.instagram.com/icegov.

Ready.gov ("Ready") Seasonal Message Campaigns The National Seasonal Preparedness Messaging Calendar and Key Messages provides content to help promote preparedness throughout the year. Visit Ready.gov/calendar. To partner with FEMA in amplifying preparedness messages to employees or the public, email fema-private-sector-communications@fema.dhs.gov.

USCIS Social Media tools provide information. These tools include Twitter channels in both English www.twitter.com/uscis and Spanish www.twitter.com/uscis_es; a Facebook page www.facebook.com/uscis; an Instagram page www.instagram.com/uscis/; a LinkedIn page www.linkedin.com/company/uscis; and a YouTube channel for hosting video content www.youtube.com/uscis.

Enforcing and Administering Our Immigration Laws

The Department is focused on smart and effective enforcement of U.S. immigration laws while streamlining and facilitating the legal immigration process. The Department has fundamentally reformed immigration enforcement, prioritizing the identification and removal of criminal aliens who pose a threat to public safety and targeting employers who knowingly and repeatedly break the law.

Employment Eligibility Verification

E-Verify is a fast and easy Internet-based service that allows employers to electronically confirm the eligibility of their employees to work in the United States. Employers must enroll in E-Verify before they can use E-Verify to confirm the employment eligibility of their newly hired employees. E-Verify is voluntary, but some employers, such as those with federal contracts or subcontracts that contain the Federal Acquisition Regulation (FAR) E-Verify clause, and employers in certain states that have E-Verify legislation, are required to use E-Verify as a condition of contracting or business licensing. E-Verify provides manuals, guides, videos, webinars, and several other resources online in English, Spanish, and other languages for E-Verify participants and employers interested in enrolling in the program. E-Verify also provides webinars and your organization may request an E-Verify speaker for your next event. For more information on E-Verify visit www.dhs.gov/e-verify or www.uscis.gov/espanol/e-verify, friend us on Facebook at www.facebook.com/uscis, follow us on Twitter at www.twitter.com/uscis, subscribe to our e-newsletter, E-Verify Connection, view our blog, email e-verify@dhs.gov or call E-Verify Customer Support 888-464-4218.

Form I-9, Employment Eligibility Verification, is used to verify the identity and employment authorization of employees in the United States. Since November 6, 1986, employers are required to complete a Form I-9 and examine documentation for each new U.S. hire. In 2011, USCIS launched I-9 Central, an online resource center dedicated to Form I-9. USCIS launched a Spanish version of the I-9 Central website in October 2012. This free, easy-to-use website gives employers and employees one-click access to resources, tips and guidance to properly complete Form I-9 and better understand the Form I-9 process. I-9 Central complements the M-274, Handbook for Employers, Guidance for Completing Form I-9, which is also available in Spanish. USCIS also offers free webinars about Form I-9. For more information, visit www.uscis.gov/i-9central or email I-9Central@dhs.gov or call 888-464-4218.

Self-Check is a free online service of E-Verify that allows U.S. workers to confirm their own employment eligibility. It is the first online verification service offered directly to workers. Available in English and Spanish, Self-Check enables individuals to enter information into Self-Check that employers would enter into E-Verify. If a problem exists with their records related to employment eligibility, Self-Check explains how to resolve that issue. Job seekers are encouraged to use Self-Check to make sure their records are in order. The Self-Check site also has an information tool kit with materials that can be distributed to increase awareness of the service. For more information on Self-Check, please visit www.uscis.gov/selfcheck or www.uscis.gov/selfcheck/espanol, email everifyselfcheck@dhs.gov, or call 855-804-0296.

Employment Eligibility Verification Program Webinars are live Internet-based seminars offered to the public on Form I-9, E-Verify Overview, E-Verify for Existing Users, E-Verify for Federal Contractors, and Self Check. Monthly webinars are scheduled on each topic and USCIS can customize webinars for associations and large employers. For more information and to see the schedule of webinars, visit the webinar page on www.dhs.gov/e-verify or email e-verify@dhs.gov.

Verification Programs Videos are available to help employers use E-Verify in a fair and non-discriminatory manner and in full compliance with their responsibilities under the terms of use. The videos, produced jointly by CRCL and USCIS, are available online at: www.uscis.gov/everify. Written pamphlets accompany the videos and serve as helpful desktop reminders. You may order (at no cost) the DVD videos and written pamphlets by contacting the DHS Office for Civil Rights and

Civil Liberties at crcl@hq.dhs.gov.

Immigration Enforcement

Carrier Liaison Program (CLP) provides standardized training and assistance to international air carriers related to admissibility and fraudulent document detection to encourage carrier compliance with U.S. immigration laws. For more information, visit www.cbp.gov/travel/travel-industry-personnel/carrier-liaison-prog or contact clp@cbp.dhs.gov.

Electronic System for Travel Authorization (ESTA) is an automated system that determines the eligibility of visitors to travel to the U.S. under the Visa Waiver Program. The ESTA application collects the same information collected on Form I-94W (Nonimmigrant Visa Waiver Arrival/Departure Record). ESTA applications must be submitted at least 72 hours prior to travel, though it is recommended that travelers apply when they begin preparing travel plans. Travelers participating in this program are required to pay a $14.00 travel fee with their ESTA application. For more information, see https://esta.cbp.dhs.gov/ or contact 202-344-3710.

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

Project CAMPUS Sentinel ICE's Student and Exchange Visitor Program (SEVP) and CTCEU work together to identify and prevent visa abuse by school officials and students. In 2012 CTCEU initiated an outreach program directed at SEVP-certified schools. The Project Campus Sentinel focuses on opening communication channels directly between designated schools officials (DSOs) and HSI special agents in ICE field offices. Through this outreach, CTCEU's goal is to build partnerships between ICE field offices and SEVP-certified schools to detect and combat school fraud and visa exploitation. Project Campus Sentinel not only provides school officials with the tools to help them identify possible threats to national security within the F and/or M student population, but also provides them with the proper outlet to report this information. So far, HSI special agents have made more than 1,200 outreaches in all 50 states, Puerto Rico and Guam For more information, visit www.ice.gov/counterterrorism-and-criminal-exploitation-unit or https://studyinthestates.dhs.gov/2013/03/designated-school-officials-what-is-campus-sentinel.

The Student and Exchange Visitor Program (SEVP) was established in 2003 to balance national security concerns with facilitating eligible nonimmigrant student and exchange visitor participation in America's outstanding academic and cultural exchange programs. SEVP exemplifies our commitment to open doors and secure borders by facilitating the process for millions of welcomed students and exchange visitors while closing loopholes for those wishing to defraud our systems or do us harm. On behalf of DHS, SEVP manages schools, nonimmigrant students in the F and M visa classifications, and their dependents. The Department of State (DoS) manages Exchange Visitor Programs, nonimmigrant exchange visitors in the J visa classification, as well as their dependents. Both SEVP and the DoS use SEVIS to track and monitor schools, exchange visitor programs, and F, M and J nonimmigrants while they visit the United States and participate in the U.S. education system. SEVIS provides timely data to the Department of State, Department of Justice, CBP, USCIS, and ICE. For more information, visit www.ice.gov/sevis or contact the SEVP Response Center at 703-603-3400.

Study in the States is managed by SEVP and is a resource for international students and school officials. It is part of a DHS initiative to enhance national security and improve customer service tied to regulations governing international students studying in the United States. Study in the States clearly explains the student visa process, enhances coordination among government agencies, and keeps international students and the U.S. academic community better informed about pertinent rules and regulations. This initiative brings together SEVP, USCIS, CBP, and the Department of State's Bureau of Consular Affairs and Bureau of Educational and Cultural Affairs. For more information, visit http://studyinthestates.dhs.gov or contact

the SEVP Response Center at 703-603-3400.

Immigration Guidance

A Guide to Naturalization contains information about the naturalization process, laws and regulations. For more information, see www.uscis.gov/files/article/M-476.pdf.

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

USCIS Report Fraud page on the USCIS website provides information on how to report fraud related to immigration benefits such as marriage or asylum fraud, as well as employment-based visa violations. See www.uscis.gov/report-fraud.

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

USCIS Information for Employers and Employees is a website regarding the employment authorization verification process and the immigration petition process. Please visit www.uscis.gov and click on 'Information for Employers and Employees' under 'Learn about working in the U.S.'. For more information contact public.engagement@dhs.gov.

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

USCIS Resources USCIS offers a variety of resources including guides, videos, citizenship toolkits, an immigration law glossary, reports and studies, civics and citizenship education resources, and a historical library. See the "Resources" section at /www.uscis.gov. USCIS has also made all our public use applications and petitions available on our website. Customers can immediately access forms from a computer, download and save the forms, fill them in electronically, and print them on demand. See the "Forms" section at www.uscis.gov. For more information contact public.engagement@dhs.gov.

Visa Waiver Program (VWP) enables citizens and nationals from selected countries to travel to and enter the United States for business or tourism for up to 90 days without obtaining a visa. For more information about the Visa Waiver Program, please visit www.cbp.gov/travel/international-visitors/visa-waiver-program.

Immigration Questions and Concerns

Office of the Citizenship and Immigration Services Ombudsman (CIS Ombudsman) Annual Reports to Congress focus on identifying systemic issues in granting immigration benefits as well as pervasive and serious problems faced by individuals and employers in their interactions with USCIS. The Annual Report contains cumulative analysis and recommendations and provides details on activities undertaken by the Ombudsman during the calendar year. For more information, see www.dhs.gov/files/publications/gc_1301971419354.shtm#1

CIS Ombudsman Updates share information on current trends and issues to assist individuals and employers in resolving potential problems with USCIS. For more information, see www.dhs.gov/xfoia/gc_1306427283101.shtm.

CIS Ombudsman Teleconferences provide an opportunity to discuss the public's interactions with USCIS and share comments, thoughts, and suggestions as well as any issues of concern. For more information, including questions and answers from previous teleconferences and a schedule of upcoming calls, visit

www.dhs.gov/files/programs/gc_1171038701035.shtm To participate in these calls, please RSVP to cisombudsman.publicaffairs@hq.dhs.gov specifying which call you would like to join. Participants will receive a return email with the call-in information.

CIS Ombudsman Recommendations are intended to ensure national security and the integrity of the legal immigration system, increase efficiencies in administering citizenship and immigration services, and improve customer service in the rendering of citizenship and immigration services. Trends reported to the Ombudsman by individuals and employers (through casework and public engagements) provide the basis for many of the recommendations. The Ombudsman is dedicated to identifying systemic problems in the immigration benefits process and preparing recommendations for submission to U.S. Citizenship and Immigration Services (USCIS) for policy and process changes. www.dhs.gov/files/publications/editorial_0769.shtm.

Submit a Request for Case Assistance to the CIS Ombudsman if you are experiencing a problem related to an immigration benefit with USCIS. To submit a case problem on behalf of somebody other than yourself, you should ensure that the person the case problem is about (the applicant for a USCIS immigration benefit, or the petitioner who seeks to obtain an immigration benefit for a third party) consents to your inquiry (see Submitting a Case Problem using DHS Form 7001: Section 15 Consent). For more information, see www.dhs.gov/files/programs/editorial_0497.shtm.

Ensuring Resilience to Disasters

The Department of Homeland Security provides the coordinated, comprehensive federal response in the event of a terrorist attack, natural disaster or other large-scale emergency while working with federal, state, local, and private sector partners to ensure a swift and effective recovery effort. The Department builds a ready and resilient nation through efforts to: bolster information sharing and collaboration, provide grants, plans and training to our homeland security and law enforcement partners, facilitate rebuilding and recovery along the Gulf Coast in impacted communities.

Business Preparedness

Business Continuity Planning Suite Critical Manufacturing SSA developed an introductory *Business Continuity Planning Suite* to assist small- to medium-sized companies reduce the potential impact of a disruption to business. The Suite includes Business Continuity Planning Training, Business Continuity and Disaster Recovery Plan, Generators, and a Business Continuity Plan Validator. For more information, see www.ready.gov/business-continuity-planning-suite.

FEMA National Continuity Programs: Policy, Plans, and Evaluation Division supports the nation's resiliency capabilities by coordinating the development and promulgation of continuity policies, plans, training, and exercises to ensure that the whole community, federal, state, local, tribal, territorial government jurisdictions, non-governmental organizations, and private sector critical infrastructure owners and operators are prepared to sustain National Essential Functions and provide critical services to the nation at all times, under all conditions. For more information, visit www.fema.gov/continuity-resource-toolkit or email fema-cgc@fema.dhs.gov.

National Business Emergency Operations Center (NBEOC) is FEMA's virtual clearing house for two-way information sharing between public and private sector stakeholders in preparing for, responding to, or recovering from disasters. Participation in the NBEOC is open to all members of the private sector. During response activities, NBEOC members are linked into FEMA's National Response Coordination Center (NRCC), activated Regional Response Coordination Centers (RRCCs), and the broader network of emergency management operations to include our state and federal partners. For more information on joining, please email us at fema-private-sector@fema.dhs.gov or visit www.fema.gov/nbeoc.

National Earthquake Hazards Reduction Program (NEHRP) FEMA created the *QuakeSmart* program as part of NEHRP to help local businesses mitigate earthquake losses and get back up and running as quickly as possible after a disaster. Among other resources, FEMA has developed the *QuakeSmart* toolkit (FEMA P811 Earthquake Publications for Businesses), which contains actionable and scalable guidance and tools for the private sector, owners, managers, and employees that emphasizes the importance of earthquake mitigation and the simple things they can do to reduce the potential of earthquake damages, injuries, and financial losses. For more information, see www.fema.gov/quakesmart.

Public Transportation Emergency Preparedness Workshop brings mass transit and passenger rail agency security and emergency management officials together with federal, state, local, and tribal government representatives and the local law enforcement and first responder community to discuss security prevention and response efforts and ways to work together to prepare and protect their communities. The two-day, invitation only, workshops enable the participants to apply their knowledge and experiences to a range of security and emergency response scenarios. For more information, see www.ntionline.com/connecting-communities-public-transportation-emergency-preparedness-workshop/ or contact masstransitsecurity@dhs.gov.

Ready Business helps owners and managers of small- and medium-sized businesses prepare their employees, operations and assets in the event of an emergency. For free tools and resources, including how to create a business emergency plan, please visit www.ready.gov.

The National Integration Center Technical Assistance (NIC TA) Program provides specialized expertise and services to state,

local, tribal, and territorial partners to improve emergency management capabilities. NIC TA support includes self-guided resources for all jurisdictions, including planning guidance, templates and checklists, and interactive support for targeted jurisdictions based on greatest need, risk, and national priorities. For more information, visit www.fema.gov/fema-technical-assistance-program or email fema-tarequest@fema.dhs.gov.

PrepTalks are video presentations given by subject-matter experts and thought leaders to spread new ideas, spark conversation, and promote innovative leadership for the issues confronting emergency managers now and over the next 20 years. Each PrepTalk release includes a video of the presentation and the question-and-answer session, a facilitator guide and discussion points, and additional resources for the topic. For a full list of PrepTalks, visit www.fema.gov/preptalks.

Emergency Communications

Wireless Emergency Alerts (WEA) is a public safety system that allows customers who own certain wireless phones and other compatible mobile devices to receive geographically-targeted, text-like messages alerting them of imminent threats to safety in their area. For more information, see www.fema.gov/frequently-asked-questions-wireless-emergency-alerts#.

Communications Sector Specific Plan (COMM SSP) involves CS&C in partnership with government and private sector communications members to ensure the Nation's communications networks and systems are secure, resilient and rapidly restored after an incident. Communications SSP is available at www.dhs.gov/publication/nipp-ssp-communications-2015. For more information, contact comms_sector@hq.dhs.gov.

The Continuity Guidance Circular (CGC) guides whole community efforts to develop and maintain the capability to ensure continuity of operations, continuity of government, and enduring constitutional government during an emergency that disrupts normal operations. The Circular describes federal and non-federal continuity efforts; outlines whole community continuity roles, responsibilities, and coordinating structures; and describes the process for building and maintaining capabilities to ensure the performance of essential functions and delivery of critical services and core capabilities. The document is available in both English and Spanish at: www.fema.gov/continuity-guidance-circular-cgc.

Emergency Alert System (EAS) is a national public warning system that requires TV and radio broadcasters, cable television systems, wireless cable systems, satellite digital audio radio service providers, direct broadcast satellite service providers and wireline video service providers to offer to the President the communications capability to address the American public during a national emergency. The system is also frequently used by state and local authorities, and the National Weather Service to deliver important emergency information such as evacuation notices, AMBER (missing children) alerts and emergency weather information targeted to a specific area. For more information, see www.fema.gov/emergency-alert-system.

Emergency Communications Guidance Documents and Methodologies are stakeholder-driven guidance documents and methodologies to support emergency responders across the nation as they plan for and implement emergency communications initiatives. These resources identify and promote best practices for improving statewide governance, developing standard operating procedures, managing technology, supporting training and exercises, and encouraging use of interoperable communications. For more information, please visit www.dhs.gov/cisa/emergency-communications.

Emergency Data Exchange Language (EDXL) messaging standards help emergency responders exchange critical data, including alerts, hospital capacity, and availability of response personnel and equipment. The National Incident Management System Supporting Technology Evaluation Program (NIMS STEP) evaluates the adherence of products to the EDXL suite of standards. IPAWS uses the EDXL Common Alerting Protocol (CAP) information standard to exchange alert and warning messages across many technologies and communications industry interfaces. NIMS STEP provides industry with an independent third-party evaluation of products, devices, systems, and data management tools – including off-the-shelf hardware and software – that support emergency managers and responders in

decision making prior to, and during, emergency operations. Evaluation activities are designed to help expand technology solutions and provide the emergency management/response community with a comprehensive process to assist in the purchasing of incident management products. For more information on the EDXL standards, see www.oasis-open.org. For NIMS STEP see, www.fema.gov/media-library-data/20130726-1744-25045-6830/101006nimsstep.pdf.

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

Integrated Public Alert and Warning System (IPAWS) is the nation's alert and warning infrastructure. IPAWS connects authorized public safety officials to the Emergency Alert System (EAS), Wireless Emergency Alerts (WEA), the National Oceanic and Atmospheric Administration (NOAA) Weather Radio network, and other public communications systems that can deliver emergency information to people from a single interface. More than 1,400 local, state, federal, territorial and tribal agencies, use Common Alerting Protocol (CAP) compliant tools to interface with IPAWS to send alerts to cell phones, radio, TV, NOAA Weather Radios, and other Internet connected devices. See www.fema.gov/ipaws.

The **National Council of Statewide Interoperability Coordinators (NCSWIC)**, managed by the Office of Emergency Communications (OEC), was established to assist state and territory interoperability coordinators with promoting the critical importance of interoperable communications and the sharing of best practices to ensure the highest level of interoperable communications is achieved for America's first responders and the individuals they are providing services to. The NCSWIC members are enhancing the response capabilities of public safety responders by coordinating and collaborating with federal, state, local, tribal and non-governmental public safety and public safety responder agencies. For more information contact OEC@hq.dhs.gov.

National Emergency Communications Plan (NECP) sets goals and identifies key national priorities to enhance governance, planning, technology, training, exercises, and disaster communications capabilities. The NECP establishes specific national priorities to help state and local jurisdictions improve communications interoperability by adopting a series of goals and milestones that measure interoperability achievements over a period of years beginning in 2008. For more information, see www.dhs.gov/files/publications/gc_1217521334397.shtm or contact the Office of Emergency Communications, oec@hq.dhs.gov.

National Interoperability Field Operations Guide (NIFOG) is a technical reference for radio technicians responsible for radios that will be used in disaster response applications, and for emergency communications. The NIFOG includes rules and regulations for use of nationwide and other interoperability channels, frequencies and channel names, and other reference material, formatted as a pocket-sized guide for radio technicians. The NIFOG can be accessed online at www.dhs.gov/safecom/resources. For more information, please contact the Cybersecurity and Infrastructure Security Agency at nifog@hq.dhs.gov.

National Security Telecommunications Advisory Committee (NSTAC) Recommendations address national security and emergency preparedness issues from a private sector perspective and reflects over a quarter century of private sector advice to the president and the nation. Issues include network convergence, network security, emergency communications operations, resiliency and emergency communications interoperability. NSTAC recommendations can be found at www.dhs.gov/cisa/nstac-publications. For more information, contact nstac@dhs.gov.

Risk Communication Best Practices and Theory Guides Effective risk communication requires a strong understanding of complex factors including trust between the communicator(s) and the audience(s), cognitive involvement and uncertainty of the

audience, cost reward tradeoffs, emotional responses to risk, and understanding and acknowledging diverse audiences. The National Consortium for the Study of Terrorism and Responses to Terrorism (START), a DHS Emeritus Center of Excellence, with sponsorship from the DHS Science and Technology Directorate, developed and evaluated a program to train local leaders on effective risk communication practices related to homeland security threats. The training program reflects the current scientific understanding of effective communication of threats and risk related to preparedness, warnings of imminent threats, and post-event recovery and mitigation. Research reports are available online, including Understanding Risk Communication Theory: A Guide for Emergency Managers and Communicators and Understanding Risk Communication Best Practices: A Guide for Emergency Managers and Communicators, as well as an accompanying Executive Summary and Appendices. For more information on this Center of Excellence, contact universityprograms@hq.dhs.gov.

SAFECOM Guidance on Emergency Communications Grants provides recommendations to grantees seeking funding for interoperable emergency communications projects, including allowable costs, items to consider when funding emergency communications projects, grants management best practices for emergency communications grants, and information on standards that ensure greater interoperability. The guidance is intended to ensure that federally-funded investments are compatible and support national goals and objectives for improving interoperability nationwide. For more information, please visit www.dhs.gov/safecom/funding.

SAFECOM Program is a public safety-driven communications program managed by the Emergency Communications Division (ECD). Through collaboration with emergency responders and policymakers across all levels of government, the SAFECOM Program works to improve multi-jurisdictional and intergovernmental communications interoperability. Its membership includes more than 65 members representing state, local, and tribal emergency responders, and major intergovernmental and national public safety associations, who provide input on the challenges, needs, and best practices involving emergency communications. Find more information at: www.dhs.gov/safecom.

Government Emergency Telecommunications Service (GETS) During emergencies, the public telephone network can experience congestion due to increased call volumes and/or damage to network facilities, hindering the ability of first responders, national security, and emergency preparedness and response personnel to complete calls. GETS provides these essential personnel priority access and prioritized processing in the local and long-distance segments of the landline networks, greatly increasing the probability of call completion. GETS is intended to be used in an emergency or crisis when the network is congested and the probability of completing a normal call is reduced. For more information, please visit www.dhs.gov/cisa/government-emergency-telecommunications-service-gets.

Telecommunications Service Priority (TSP) Program authorizes national security and emergency preparedness (NS/EP) organizations to receive priority treatment for vital voice and data circuits. The TSP program provides service vendors a Federal Communications Commission mandate to prioritize requests by identifying those services critical to NS/EP. NS/EP services are those used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or degrades or threatens the NS/EP posture of the United States. For more information, please visit www.dhs.gov/cisa/telecommunications-service-priority-tsp or contact support@priority-info.com.

Voice over Internet Protocol (VoIP) Project researches IP-enabled communication technologies and evaluates promising solutions. This project enables the emergency response community to confidently deploy and use IP technologies and integrate video, cellular, and satellite communications. The project will complete the development of a set of standards based on the needs of emergency responders. For more information, see www.pscr.gov/projects/broadband/voip/voip.php, or contact voip_working_group@sra.com.

Wireless Priority Service (WPS) provides national security and emergency preparedness personnel with priority access and prioritized processing in all nationwide and several regional cellular networks, greatly increasing

the probability of call completion. WPS is intended to be used in an emergency or crisis when cellular networks are congested and the probability of completing a normal cellular call is reduced. WPS is an easy-to-use, add-on feature subscribed to on a per-cell phone basis. It is deployed by cellular service providers throughout the United States. WPS calls will receive priority over normal cellular calls; however, WPS calls do not preempt calls in progress or deny the general public's use of cellular networks. WPS is in a constant state of readiness. For more information, please visit www.dhs.gov/cisa/about-wps.

Emergency Responder Community

The Emergency Services Sector Cybersecurity Initiative is an ongoing effort to enable the Emergency Services Sector (ESS) to better understand and manage cyber risks and to coordinate the sharing of cyber information and tools between subject matter experts (both inside and outside the federal government) and the ESS disciplines. Contact essteam@hq.dhs.gov for more information.

Crisis Event Response and Recovery Access (CERRA) The capability for state, local, tribal, and territorial authorities to safely, securely, and effectively control and coordinate the access of key response and recovery resources into an affected area during an emergency has been identified as a critical success factor in enabling overall community recovery. The CERRA Framework focuses on supporting state, local, tribal, and terrirotial efforts to enable the successful transit and access of critical response and recovery resources before, during, and after emergencies. Contact essteam@hq.dhs.gov for more information.

Emergency Services Sector – Continuity Planning Suite (ESS-CPS) provides a centralized collection of existing guidance, processes, products, tools, and best practices to support the development and maturation of continuity planning for the first responder community. ESS-CPS was created through a partnership of the Emergency Services Sector-Specific Agency (SSA) and Sector Coordinating Council (SCC). First responders can use the ESS-CPS as it suits their organization to evaluate and improve their continuity capability and enhance their preparedness for emergencies. Contact essteam@hq.dhs.gov for more information.

AUXCOMM Training Auxiliary communicators (amateur radio operators) have supported state/local public safety agencies for decades during natural disasters and other emergencies. Cybersecurity and Infrastructure Security Agency (CISA) technical assistance offers a training course for auxiliary communicators volunteering their services under the auspices of a public safety agency. This two-day training course is for those amateur radio operators who wish to volunteer to support public safety during emergencies and integrate into a National Incident Management System Industrial Control Systems Communications Unit function. For information, individuals should see the CISA Technical Assistance/Statewide Communications Interoperability Plan Guide posted at: www.dhs.gov/ictapscip-resources.

For further information, contact comu@hq.dhs.gov.

AgConnect is a suite of customizable data integration and analysis products designed to enhance situational awareness and support decision-making for emerging, zoonotic and/or transboundary animal diseases. The tool was developed under the Institute for Infectious Animal Diseases, co-lead for the DHS Emeritus Center of Excellence for Zoontic and Animal Disease Defense in partnership with the Texas Center for Applied Technology, a part of the Texas A&M Engineering Experiment Station. The technology integrates authoritative information from disparate sources into a single, easy-to-use integrated display. It empowers real-time collection, access, distribution and analysis of bio-surveillance, veterinary diagnostic, animal movements and other pertinent data (e.g., clinical observations, production information, genetics and environmental/climate data). These data are integrated into an interoperable, permissioned, user-defined operational picture that allows users to make decisions based on common information that can be shared across echelons, organizations, locations and roles/positions. For more information, see https://iiad.tamu.edu/agconnect/ or AgConnect® Overview. For more information on this Center of Excellence, contact universityprograms@hq.dhs.gov.

Center for Domestic Preparedness (CDP) offers several interdisciplinary programs that are designed for those with emergency response and healthcare responsibilities, or who meet the criteria specified in the website

mentioned below. CDP offers courses in chemical, biological, radiological, nuclear, and explosive incident response, toxic agent training, and healthcare response for mass casualty incidents, Radiological Emergency Preparedness Program courses, field force operations, and incident command. CDP is home to the only facility where civilian responders can train in a toxic agent environment using both chemical and biological agents—the Chemical, Ordnance, Biological, and Radiological Training Facility (COBRATF). The CDP's healthcare courses include exercises in the nation's only hospital facility dedicated solely to preparedness and mass casualty response training—the Noble Training Facility (NTF). CDP training is free for state, local, and tribal agencies; round-trip air and ground transportation, lodging, and meals are provided at no cost to responders or their agency. Federal, private sector, and international agencies are encouraged to attend on a space available basis, but they must pay a tuition fee for the courses in addition to transportation, meals and lodging fees. For more information, see https://cdp.dhs.gov/find-training or call 866-213-9553.

Cybersecurity in the Emergency Services Sector The one-hour course will provide an overview of the types of cyber systems and infrastructure that the Emergency Services Sector utilizes; and address the threats and vulnerabilities to those cyber resources. The webinars are available on the Homeland Security Information Sharing – Critical Sectors Emergency Services Sector portal. For access and more information, contact the Cybersecurity and Infrastructure Security Agency's Infrastructure Security Division Emergency Services Sector at essteam@hq.dhs.gov.

DHS Center of Excellence: Coastal Resilience Center (CRC), led by the University of North Carolina at Chapel Hill in partnership with Jackson State University in Mississippi, conducts research and education to enhance the nation's ability to safeguard people, infrastructure, and economies from catastrophic coastal natural disasters such as floods and hurricanes. Resources include the ADCIRC Prediction System for storm surge and coastal flooding and the Plan Integration for Resilience Scorecard (PIRS) for community hazard vulnerability reduction. For more information, visit https://coastalresiliencecenter.unc.edu/, or contact universityprograms@hq.dhs.gov.

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

Emergency Services Personal Readiness Guide for Responders and Their Families is a tri-fold handout providing a description of the Ready Campaign and the Emergency Services Sector-Specific Agency, and provides a list of website resources and instructions on family preparedness. Specifically, suggestions on developing an emergency kit and family emergency plan. For more information, or to request materials contact the Emergency Services Sector-Specific Agency at ESSTeam@hq.dhs.gov.

Emergency Services Sector (ESS) Video This is a three-minute video providing an overview of the ESS Sector. The video is appropriate for conferences and events to grow awareness and participation in sector activities. For more information, contact ESSTeam@hq.dhs.gov.

Emergency Services Self-Assessment Tool (ESSAT) is a secure, web-based application that enables public and private entities to perform risk assessments of specialized assets and systems, as well as multiple systems in a particular region, through voluntary and interactive stakeholder involvement. It allows for a coordinated effort among sector partners by collecting and sharing common risk gaps, obstacles, and protective measures. The tool benefits individual partners and collective disciplines and supports sector-wide risk management efforts. For more information, please contact the Emergency Services SSA at ESSTeam@hq.dhs.gov.

FEMA Higher Education Program The primary goal of the FEMA Higher Education Program is to work with colleges and universities, emergency management professionals, and stakeholder organizations to help create an emergency management system of sustained, replicable capability and disaster loss reduction through formal education, experiential learning, practice, and experience centered on mitigation, preparedness, response and recovery from the full range of natural, technological and intentional hazards which confront

communities across the Nation. For more information, select the following link: https://training.fema.gov/hiedu/.

FEMA Emergency Management Institute (EMI) Independent Study Program (ISP) offers self-paced courses designed for those with emergency management responsibilities, as well as for the general public. The FEMA Independent Study Program offers courses that support the five mission areas identified by the National Preparedness Goal: prevention, protection, mitigation, response, and recovery. For more information on EMI training courses, please visit https://training.fema.gov/IS/ or contact us 301-447-1200.

FEMA Emergency Management Institute Programs offers several programs that are designed for those with emergency management responsibilities or meet the criteria specified at the website cited below. The training is free of charge, but individuals from the private sector or contractors to state, local or tribal governments must pay their own transportation and lodging fees. EMI has an integrated training approach and encourages individuals from the private sector to participate in its courses. EMI programs include, but are not limited to, the Master Exercise Practitioner Program, the Emergency Management Professional Program (EMPP), the Applied Practices Series and the Public Information Officer Training Program. For more information, see https://training.fema.gov/Programs/ or call 301-447-1286.

FEMA National Emergency Training Center (NETC) provides current information and resources on fire, emergency management and other all-hazards subjects. With its collection of more than 180,000 books, reports, periodicals, and audiovisual materials, the NETC Library houses the most extensive collection of fire service literature in the U.S. The NETC Library collection of books and research reports may also be accessed by requesting interlibrary loan through a local library. For more information contact netclrc@fema.dhs.gov or 1-800-638-1821.

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

First Responder Communities of Practice is an online network of vetted, active, and retired first responders, emergency response professionals and federal, state, local, and tribal and territorial homeland security officials. Registered members of this professional network share information, ideas, and best practices, enabling them to more efficiently and effectively prepare for all hazards. See www.firstresponder.gov or www.dhs.gov/publication/first-responder-communities-practice

First Responders 'Go Kit' This video is designed to demonstrate step-by-step what First Responders should have in their personal and family emergency kit. For more information please contact the Emergency Services SSA at essteam@hq.dhs.gov.

National Level Exercise (NLE) 2020 will involve a complex, adversary-based multidimensional attack that reflects the evolving threat environment. This exercise series will examine a complex threat that originates overseas. Widespread cyberattacks result in a domestic national security emergency involving significant impacts to multiple critical infrastructure sectors. Partners across the whole community, including all levels of government, the private sector, nongovernmental organizations, and community groups will participate in NLE 2020. Lead-up preparedness events will commence in 2019 and the functional and full-scale components of the exercise series will occur from February through May 2020. For more information, visit https://portalapps.fema.net/apps/PNP-NED/HSIP/Pages/NationalLevelExerciseSection.aspx.

National Training and Education Division (NTED) courses are delivered in a variety of formats including web-based, resident, and non-resident. NTED draws upon a diverse group of training providers, also referred to as training partners, to develop and deliver NTED approved training courses. These training providers include the National Domestic Preparedness Consortium (NDPC), the Rural Domestic Preparedness Consortium (RDPC), and the Naval Postgraduate School

(NPS), and Continuing Training Grants Partners. For more information, visit www.firstrespondertraining.gov or contact firstrespondertraining@fema.dhs.gov or 1-800-234-1116.

The R-Tech Bulletin is a publication on technologies of interest to first responders who have received funding, in part, from the federal government. Interested individuals can subscribe to the bulletin by RSS feed or can download the bulletin at www.firstresponder.gov/pages/newsletter.aspx .

Safety and Security of Emergency Response Vehicles Brochure This brochure outlines and recommends how to keep emergency response vehicles and equipment safe form theft incidents. Emergency responders will know how to prevent the loss of property by actively enforcing effective theft prevention measures. For more information, please contact the Emergency Services SSA at essteam@hq.dhs.gov.

Technologies for Critical Incident Preparedness (TCIP) Conference and Exposition highlights DOJ, DHS, and DoD technologies; Research, Development, Testing & Evaluation investments; and training tools for the emergency responder community. It provides a forum for emergency responders to discuss best practices and exchange information and offers a unique opportunity for emergency responders; business and industry; academia; federal and state, local, tribal, and territorial stakeholders to network, exchange ideas, and address common critical incident technology, preparedness, response and recovery needs, protocols, and solutions. For more information, see www.tcipexpo.com.

Video Quality in Public Safety (VQiPS) Working Group was formed to focus on the major policy, technology, and practical uses and challenges of public safety video systems. Comprised of emergency responders, academics, federal partners, and vendors, the working group developed an end-user guide to help practitioners articulate their needs to vendors when they look to purchase or upgrade video systems. For more information, see www.dhs.gov/science-and-technology/voice-video-and-data-public-safety or contact vqips@hq.dhs.gov.

Webinar: The Ready Responder Program for the Emergency Services Sector The one-hour web-based seminar focuses on first responder preparedness and best practices and how the Ready Responder program contributes to a safer, more secure and more resilient America. The webinars are available on the Homeland Security Information Sharing – Critical Sectors Emergency Services Sector portal. For access and more information, contact the Emergency Services Sector at essteam@hq.dhs.gov.

Personal and Community Preparedness

American Wood Council: The U.S. Fire Administration (USFA) in partnership with the American Wood Council (AWC) developed a web-based educational program for the fire service on modern construction components and technology. The web-based program provides information on the structural use of traditional and engineered wood products in modern construction, including trusses, structural glued laminated timber beams, I-joists, structural composite lumber, structural insulated panels and wood structural panels. For more information, see Woodaware.info.

Are You Ready? An In-depth Guide to Citizen Preparedness provides a step-by-step approach to disaster preparedness, including specific hazard-based activities Americans of any age can take. For more information see www.ready.gov or call 800-480-2520 to order materials. Questions regarding the Individual and Community Preparedness can be directed to FEMA-Prepare@fema.dhs.gov

Assistance to Firefighters Grants (AFG) works to enhance the safety of the public and firefighters with respect to fire-related hazards by providing direct financial assistance to eligible fire departments, non-affiliated Emergency Medical Services organizations, and State Fire Training Academies. This funding is for critically needed resources to equip and train emergency personnel to recognized standards, enhance operations efficiencies, foster interoperability, and support community resilience. For additional information, see: www.fema.gov/welcome-assistance-firefighters-grant-program.

Building a Roadmap to Resilience - A Whole Community Training is a 3-day course that helps communities build a Whole Community approach to emergency management by teaching principles, themes, and pathways for

action, and other promising practices uncovered by local leaders across the nation. Participants will develop a plan of implementation in their own community, receive the tools and knowledge to establish a community coalition, and learn to encourage local leaders to augment resilience within the unique circumstances of their community. For more information, see www.firstrespondertraining.gov and search "Roadmap to Resilience".

Community Emergency Response Team (CERT) helps train citizens to better prepare for and respond to emergency situations in their communities. When emergencies happen, CERT members can give critical support to first responders, provide immediate assistance to survivors, and organize spontaneous volunteers at a disaster site. CERT members can also help with non-emergency projects that help improve the safety of the community. There are CERT programs in more than 2,700 communities across the nation. For more information, visit www.ready.gov/cert or contact fema-prepare@fema.dhs.gov.

Community Preparedness Training: Implementing Simple Activities for Everyone (IS-909) is an interactive or plenary course designed to help organizations conduct simple preparedness activities for their employees and/or staff. It includes a set of materials focused on areas such as local hazards, local alerts and warnings, and local community response resources and protocols that can be tailored based on the needs of training participants. For more information, see https://training.fema.gov/is/courseoverview.aspx?code=is-909.

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

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

The Emergency Food and Shelter National Board Program (EFSP) was created in 1983 to supplement the work of local social service organizations, both non-profit and governmental, within the U.S. and its territories, to help people in need of emergency economic assistance. Funding is open to all organizations helping the U.S. hungry and homeless. This collaborative effort between the non-profit and public sectors has provided over $3.6 billion in federal funds during its 28-year history.
The Emergency Food and Shelter National Board Program funding is apportioned nationally to Local Boards where it is administered and used for:

- Food, in the form of served meals or groceries.
- Lodging in a mass shelter or hotel.
- One month's rent or mortgage payment.
- One month's utility bill.
- Equipment necessary to feed or shelter people, up to a $300 limit per item.

For more information, visit http://efsp.unitedway.org.

FEMA Regulatory Materials The majority of regulations specific to FEMA are located in the Code of Federal Regulations (CFR), volume 44 "Emergency Management and Assistance." FEMA's regulations govern specific agency programs and practice and have the force and effect of law. The CFR is updated daily at www.ecfr.gov. You have an opportunity to provide input on almost every FEMA regulation before it is finalized. Regulations.gov is a multi-agency website serving as an online clearing house for materials related to FEMA rulemakings and is FEMA's official on-line comment system. The website allows the public to comment on regulations and access rules that FEMA has published in the Federal Register as well as related documents. FEMA welcomes public comments on its proposed regulatory actions. The public may comment on any posted document with an "Open Comment Period." Not all comment periods are the same length, so please keep an eye on your topics of interest. For further information and additional resources, please go to www.fema.gov/rulemaking.

Fire Prevention & Safety (FP&S) grants are part of the Assistance to Firefighters Grant program and support projects that enhance

the safety of the public and firefighters from fire and related hazards. For more information, see www.fema.gov/welcome-assistance-firefighters-grant-program.

Regarding **First Responder Safety Research and Special Studies**, the U. S. Fire Administration (USFA) carries out research and specials studies to decrease injuries and fatalities in the first responder community, to develop and evaluate new technology and to increase safety and efficiency during emergency operations. This supports USFA's mission to reduce life and economic losses due to fire and related emergencies through leadership, advocacy, coordination, and support. For more information, see www.usfa.fema.gov/operations/

The National Fire Data Center (NFDC) manages a robust program of research and special studies. Our research projects cover topics supporting firefighter and emergency responder health and safety as well as fire safety of the American public. The NFDC works with relevant federal, academic and both regional and national association partners to complete these studies and publish the reports.
Topics include:

- Operational Safety
- Natural Disasters and Non-Fire Emergencies
- Protective Equipment and Clothing
- Vehicle and Roadway Safety
- Emergency Medical Services
- Wellness & Fitness

For more information, see www.usfa.fema.gov/data/statistics/reports/.

Preparedness Grants Guidance contained in the Notice of Funding Opportunity (NOFO) for the Homeland Security Grant Program (HSGP), Emergency Management Performance Grant (EMPG) and Tribal Homeland Security Grant Program (THSGP) encourages state and tribal governments to collaborate with private sector interests to address "whole community" needs relating to emergency management and homeland security investments. The NOFOs can be found at: www.fema.gov/grants.

National Flood Insurance Program focuses on flood insurance, floodplain management and flood hazard mapping. Over 22,000 communities across the U.S. and its territories participate in the NFIP by adopting and enforcing floodplain management ordinances to reduce future flood damage. In exchange, the NFIP makes federally-backed flood insurance available to homeowners, renters, and business owners in these communities. For more information, see www.floodsmart.gov; flood insurance agents, please visit www.agents.floodsmart.gov or e-mail FLOODSMART@fema.dhs.gov

The **National Mass Care Exercise (NMCE)** is an annual, national mass care system exercise that focuses on testing our Nation's ability to respond to large-scale Mass Care events. It also focuses on establishing state-to-federal coordination systems in addition to integrating staff from key Non-Government Organizations (NGOs), faith-based organizations (FBOs), the private sector and all levels of government into an effective mass care multi-agency coordination structure. NMCE is sponsored by FEMA, the American Red Cross, and host states from across the country and has been held annually since 2012. More details can be found at www.nationalmasscarestrategy.org.

The National Mass Care Strategy provides a unified approach to the delivery of mass care services by establishing common goals, fostering inclusive collaborative planning, and identifying resource needs to build the national mass care capacity to engage the whole community including under-served and vulnerable populations. These will include planning templates, case studies, resource and hazard specific guides. The National Mass Care Strategy will focus on:

- Sheltering (including household pets)
- Feeding
- Distribution of emergency supplies
- Family reunification services
- Immediate health, emotional and spiritual health services
- Access to information

For more information, see http://nationalmasscarestrategy.org/.

The **National Fire Incident Reporting System (NFIRS)** was established in the mid-1970s and is mandated by the Federal Fire Prevention and Control Act of 1974 (Public Law (PL) 93-498, as amended) which authorizes the National Fire Data Center to gather and analyze information such as 1) the frequency, causes, spread, and extinguishment of fires; 2) injuries and deaths resulting from fires; 3) information on injuries sustained by a firefighter; and 4) information on firefighting activities. The act further authorizes USFA to develop uniform data reporting methods, and to encourage and assist federal, state, local

and other agencies in developing and reporting information. NFIRS is a reporting standard that fire departments use to uniformly report on the full range of their activities, from fire to Emergency Medical Services (EMS) to severe weather and natural disasters. This reporting allows fire departments, as well as many other government and non-government agencies, to quantify their actions and identify incident and response trends.

- Over 27,000 fire departments currently report over 28 million incidents.
- Each year the USFA compiles publicly-released incidents, collected by states during the previous calendar year, into a public database that we make available to the public free of charge. Data available includes:
    - CD 1980-1998 — Fire incidents (NFIRS version 4.1)
    - CD 1999-2003 — All incidents
    - CD 2004-2017 — Fire and hazardous materials incidents
    - DVD 2014-2017 — All incidents

Further NFIRS information may be found on the USFA web site: www.usfa.fema.gov/data/nfirs/.

NFIRS References: Guides, publications, support, etc. are resources that are all publicly available. These resources cover, in specific detail, many aspects of the NFIRS standard, such as the elaboration of rules and definitions. All of the resources listed below are designed to assist the user in understanding NFIRS data and its impact to the fire department and communities served, from the local to the national level.

- Complete Reference Guide: www.usfa.fema.gov/downloads/pdf/nfirs/nfirs_complete_reference_guide_2015.pdf
- Coding Questions Guide: www.usfa.fema.gov/downloads/pdf/nfirs/nfirs_coding_questions_2016.pdf
- NFIRSGrams: www.usfa.fema.gov/data/nfirs/support/training.html

Support for all NFIRS users, analysts, and interested individuals can be obtained by contacting the NFIRS Support Center.

- Online: www.usfa.fema.gov/data/nfirs/support/training.html
- Email: fema-nfirshelp@fema.dhs.gov.
- Telephone: 1-888-382-3827

Public Private Partnerships: An Introductory Course In December 2011, FEMA launched FEMA IS-660: Introduction to Public-Private Partnerships, the first web-based course on building public-private partnerships in emergency management. Training is offered through the EMI ISP and was designed in collaboration with both the public and private sector. It is available to anyone, but recommended for emergency management and community planners, senior-level personnel from response agencies, representatives from private-sector organizations, and federal, state, local, and tribal government agencies that may participate in collaborative continuity planning efforts. For more information, see http://training.fema.gov/is/courseoverview.aspx?code=is-660.

Public Private Partnerships: An Advanced Course, IS-662 Public-private partnerships enhance all aspects of emergency management: preparedness, protection, response, recovery, and mitigation. They do so by engaging in activities such as information sharing, emergency planning, emergency communications, and resource sharing. Building from the first course, IS600, IS-662 describes how to establish and sustain public-private partnerships, as well as how to communicate and share resources in a partnership. The course includes a checklist of common considerations when establishing a public-private partnership and a toolkit complete with a comprehensive list of web resources for the public and private sectors. For more information, see https://training.fema.gov/is/courseview.aspx?code=is-662.

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

Self-Facilitated Tabletop Exercises FEMA has developed several tabletop exercises, complete with video injects and facilitator notes. These exercises can be used as an activity at the community, organization, or partnership level.

Visit: www.fema.gov/emergency-planning-exercises.

Staffing for Adequate Fire and Emergency Response (SAFER) grant program was created to provide funding directly to fire departments and volunteer firefighter interest organizations to help increase the number of trained, "front line" firefighters available in their communities. For more information, see www.fema.gov/welcome-assistance-firefighters-grant-program.

Tornado Safety Initiative assesses building damages and identifies lessons learned after tornadoes occur; funds research on shelter design and construction standards; produces public education materials on tornado preparedness and response; and develops best practices and technical manuals on the design and construction of safe rooms and community shelters for engineers, architects, building officials, and prospective shelter owners. For more information, visit www.fema.gov/library/viewrecord.do?id=2073.

Unified Hazard Mitigation Assistance (HMA) Grant Programs present a critical opportunity to reduce the risk to individuals and property from natural hazards while simultaneously reducing reliance on Federal disaster funds. HMA programs are subject to the availability of appropriation funding or funding based on disaster recovery expenditures, as well as any directive or restriction made with respect to such funds. HMA programs include: Hazard Mitigation Grant Program, Pre-Disaster Mitigation program, Flood Mitigation Assistance program, Repetitive Flood Claims (RFC) program, and the Severe Repetitive Loss program. For more information, see www.fema.gov/hazard-mitigation-assistance.

USFA On-Duty Firefighter Fatalities The U.S. Fire Administration tracks and collects information on the causes of on-duty firefighter fatalities that occur in the United States. We conduct an annual analysis to identify specific problems so that we may direct efforts toward finding solutions that will reduce firefighter fatalities in the future. This information is also used to measure the effectiveness of programs directed toward firefighter health and safety. Additional information regarding On-Duty Firefighter Fatalities may be found at: https://apps.usfa.fema.gov/firefighter-fatalities/

USFA National Fire Department Registry provides a directory of registered fire departments and includes basic information such as address, department type, website, number of stations, and number of personnel. The program is voluntary and comprises over 27,200 registered fire departments. The purpose of the registry is to create a national database for use by the fire service and its stakeholders. The online registry page contains a look-up feature for registered fire departments, as well as a current series of National Fire Department Registry Quick Facts that show graphics and charts for various fire department data elements such as number of departments registered by state and region, department types, personnel, etc. Additional information regarding the registry may be found on the USFA web site: https://apps.usfa.fema.gov/registry/.

First Responder Safety Research and Special Studies carries out research and specials studies to decrease injuries and fatalities in the first responder community, to develop and evaluate new technology and to increase safety and efficiency during emergency operations. This supports USFA's mission to reduce life and economic losses due to fire and related emergencies through leadership, advocacy, coordination, and support. The NFDC manages a robust program of research and special studies. Our research projects cover topics supporting firefighter and emergency responder health and safety as well as fire safety of the American public. The NFDC works with relevant federal, academic and both regional and national association partners to complete these studies and publish the reports. To learn more about the NFDC's research initiatives, visit: www.usfa.fema.gov/operations/.

Building a Roadmap to Resilience - A Whole Community Training. This 3-day course helps communities build a Whole Community approach to emergency management by teaching principles, themes, and pathways for action, and other promising practices uncovered by local leaders across the nation. Participants will develop a plan of implementation in their own community, receive the tools and knowledge to establish a community coalition, and learn to encourage local leaders to augment resilience within the unique circumstances of their community. For more information, see

www.firstrespondertraining.gov and search "Roadmap to Resilience".

The primary goal of **Assistance to Firefighters Grants (AFG)** is to enhance the safety of the public and firefighters with respect to fire-related hazards by providing direct financial assistance to eligible fire departments, nonaffiliated Emergency Medical Services organizations, and State Fire Training Academies. This funding is for critically needed resources to equip and train emergency personnel to recognized standards, enhance operations efficiencies, foster interoperability, and support community resilience. For additional information, see: www.fema.gov/welcome-assistance-firefighters-grant-program.

The Supply Chain Resilience Guide provides emergency managers with recommendations and best practices on how to analyze local supply chains and work with the private sector to enhance supply chain resilience using a five-phased approach. www.fema.gov/media-library/assets/documents/178701. FEMA also released two supply-chain focused PrepTalks: "Private Sector Resilience: It's all in the Supply Chain," www.fema.gov/preptalks/sheffi; and "Aligning Public and Private Sector Supply Chains Following Disasters", www.fema.gov/preptalks/goentzel.

Youth Preparedness: Starting or getting involved with a youth preparedness program is a great way to enhance a community's resilience and help develop future generations of prepared adults. The Federal Emergency Management Agency (FEMA) offers numerous resources that can help, from card games and coloring books to school-based curriculum. For more information, please visit www.ready.gov/kids.

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 www.tsa.gov/sites/default/files/non-ssi_acstl.pdf.

AIRBUST Program provides the general public and aviation community with a forum to share information on suspicious small aircraft. An AIRBUST poster and pocket-sized laminated card display the phone number for reporting suspicious activity or low-flying aircraft, 1-866-AIRBUST (1-866-247-2878). This number rings directly to the CBP Air and Marine Operations Center (AMOC) operations floor. The two-sided laminated card displays drawings of single-and twin-engine aircraft often used to transport contraband and lists helpful information to include when calling. The AIRBUST poster is an 8.5x11" poster with the 1-866-AIRBUST (1-866-247-2878) phone number. It also lists four general items of interest that can tip off a general aviation airport employee or law enforcement official that a certain 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 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, Airlines, Airports, General Aviation, Insider Threat, International Aviation, and Security Technology. For more information, see www.tsa.gov/for-industry/aviation-security.

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 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 more information and a training video, visit

www.aopa.org/airportwatch/.

Airspace Authorizations and Waivers The TSA Airspace Authorizations Office manages the review and processing of applications received from general aviation and Unmanned Aircraft System (UAS) operators who request to enter areas of restricted airspace around Washington, D.C., major sporting events and the Disney theme parks. Waivers are also processed for certain international flights and foreign-registered aircraft overflying or operating within the United States. After TSA review and manifest vetting, airspace waiver letters are prepared and transmitted to FAA System Operations Security (AJR-2) for final review and approval. TSA also processes, vets and approves flight authorizations for Ronald Reagan Washington National Airport (DCA) Access Standard Security Program (DASSP) operators who fly to and from DCA via TSA-screened Gateway Airports. For more information, see www.tsa.gov/for-industry/general-aviation 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 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 (CCSP) 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, Certifies Cargo Screening Facilities (CCSF) and Chain of Custody Standards, a tri-fold brochure, supplemental CCSP program material with at a glance program overview of the program, a quick hits overview with impact of 100% screening, and supplemental CCSP materials. For more information, see www.tsa.gov/certified-cargo-screening-program or contact ccsp@dhs.gov or the TSA Contact Center at 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 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 www.tsa.gov/stakeholders/security-programs-and-initiatives.

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 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 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 watch list matching performed by TSA agents. Secure Flight also incorporates an expedited and integrated redress process by referring travelers who think they have been misidentified or have experienced difficulties in their air travel to the DHS Traveler Redress Inquiry Program (TRIP), a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at airports, at train stations, or crossing U.S. borders. Log on to the DHS Trip (www.dhs.gov/trip) website to initiate an inquiry. For more information, visit www.tsa.gov/stakeholders/secure-flight-program or contact the TSA Contact Center, 866-289-9673.

TSA conducts **Man-Portable Air Defense Systems (MANPADS) Outreach Programs**; such as, the Law Enforcement MANPADS Awareness Training Program specifically designed for law enforcement/first responders responding to a MANPADS attack on a commercial aircraft, and MANPADS Vulnerability Assessments at U.S. airports. In accordance with the National Aviation Security Policies: National Security Presidential Directive 47 (NSPD-47) / Homeland Security Presidential Directive 16 (HSPD-16) these are just two parts of a multi-dimensional approach to detect, deter, and defeat a MANPADS threat against civil aviation. These pieces allow TSA to help implement a Domestic Outreach Plan with efforts to mitigate or respond effectively to a MANPADS event. Personnel interested in receiving more information or training should contact manpads@tsa.dhs.gov.

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 to engage a wide spectrum of private sector establishments within their jurisdictions that manufacture, distribute, or sell products that contain home-made explosives (HMEs) and 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@hq.dhs.gov.

DHS Center of Excellence: Awareness & Location of Explosives-Related Threats (ALERT) Led by Northeastern University, ALERT conducts transformational research, technology, and educational development to characterize, detect, mitigate, and respond to explosives-related threats facing the country and the world. ALERT brings strength in designing advanced sensors; detecting weakly defined targets from a standoff distance; signal processing and sensor integration; characterizing explosives; understanding improvised explosive device detonator signatures; shock physics; and material science. For more information, see www.northeastern.edu/alert/ and http://energetics.chm.uri.edu or contact universityprograms@hq.dhs.gov.

Bomb Threat Management Planning Course is a four-hour workshop which improves participants' ability to manage 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 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 www.dhs.gov/bombing-prevention-training-courses for more information.

The **Improvised Explosive Device 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. See www.dhs.gov/cisa/office-bombing-prevention-obp.

Improvised Explosive Device Search Procedures Course: This one-day, performance-based course introduces participants to basic, low-risk search protocols and allows participants to practice an IED search of a facility, an area, and a route to reduce vulnerability and migrate the effects of IED attacks. This course is designed for public and private facility owners and operators and security staff that may be tasked with search duties during a bomb threat incident. See www.dhs.gov/cisa/office-bombing-prevention-obp for more information.

Improvised Explosive Device Threat Awareness and Detection: The Cybersecurity and Infrastructure Security Agency's Office for Bombing Prevention (OBP) 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 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 CISA's Commercial Facilities SSA at cfsteam@hq.dhs.gov.

Multi-Jurisdiction Improvised Explosive Device Security Plan (MJIEDSP): MJIEDSP is a planning and assessment program managed by the CISA OBP, consisting of a series of tabletop exercises that integrate counter-IED capability analysis, training, and planning to enhance IED prevention, protection, mitigation, and response capabilities of participating jurisdictions. MJIEDSP assists participants in identifying roles, responsibilities, and capability gaps within a multi-jurisdictional planning area in alignment with the National Preparedness Goal for Countering IEDs. To request additional information, contact the CISA Office for Bombing Prevention at obp@hq.dhs.gov.

Protective Measures Course is a one-day, performance-based course that provides participants with a basic understanding of how to identify risks and vulnerabilities to a facility, determine additional security needs for a special event or public gathering, and identify and apply physical and procedural protective measures to mitigate the threat of an IED or vehicle-borne IED (VBIED). This course is designed for public and private sector security personnel at the executive, management, and operations level. Public safety workers, emergency managers, law enforcement, and special event security personnel can also benefit from the course. For more information, please visit www.dhs.gov/cisa/office-bombing-prevention-obp.

Security and Resiliency Guide: Counter-Improvised Explosive Device Concepts, Common Goals, and Available Assistance (SRG C-IED) is intended to help stakeholders plan and implement C-IED activities within their overall public safety and emergency management approach. They can use it to understand the IED risk landscape in the U.S. and their locale, apply common IED-specific security and resiliency goals, and leverage available U.S. Government resources to build and sustain preparedness. The Cybersecurity and Infrastructure Security Agency's Office for Bombing Prevention has created four annexes to the SRG C-IED catered to specific groups, including those in the lodging industry, outdoor event sponsors, sports leagues and venues, and businesses (movie theatres, convention centers, etc.) where there is public assembly. Find the SRG C-IED and its annexes at www.dhs.gov/publication/security-and-resiliency-guide-and-annexes. For more information about bombing prevention, visit www.dhs.gov/obp or contact CISA OBP at obp@hq.dhs.gov.

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 additional information about this course, contact the Cybersecurity and Infrastructure Security Agency Office for Bombing Prevention at obp@hq.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/cisa/report-cfats-violation or contact 877-FYI-4-DHS (1-877-394-4347) or email cfatstips@hq.dhs.gov. 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 Frequently Asked Questions (FAQs) assist facilities in complying with the CFATS regulation. The FAQs are searchable and categorized to further benefit the user. Visit www.dhs.gov/cisa/chemical-facility-anti-terrorism-standards and click on "CFATS Knowledge Center." For more information, contact cfats@hq.dhs.gov or call the CFATS Help Desk at 866-323-2957.

Chemical Facility Anti-Terrorism Standards Presentations are used by CISA in discussions with the chemical industry and those interested in chemical security. If interested in a live presentation about CFATS by CISA personnel, or to find more information about such presentations, see www.dhs.gov/files/programs/gc_1224766914427.shtm or contact the CFATS at cfats@dhs.gov or 866-323-2957.

Chemical Facility Anti-Terrorism Standards 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, the Cybersecurity and Infrastructure Security Agency has developed a Risk-Based Performance Standards Guidance document which can be found at 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) is the nation's only federal study, analysis, and knowledge-management center for assessing the threat and hazard associated with an accidental or intentional large-scale chemical event or chemical terrorism event in the U.S. CSAC provides an enduring science-based threat and risk analysis capability with a core focus on chemical risk and consequence modeling, analytical chemistry, chemical toxicology, synthetic chemistry, and chemical informatics. CSAC serves the broader Homeland Security Enterprise and stakeholders by maintaining a Technical Assistance program staffed and available 24/7 to provide operational support and subject matter expertise, designing and executing laboratory and field tests, and providing a comprehensive knowledge repository of chemical threat information that is synthesized and continuously updated with data from scientific, intelligence, operational, and private sector sources. For more information, contact the CSAC at csacinfo@st.dhs.gov or 410-417-0910.

Chemical Security Assessment Tool (CSAT) is an online tool developed by the Cybersecurity and Infrastructure Security Agency 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 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 Cybersecurity and Infrastructure Security Agency upon request by Chemical Facility Anti-Terrorism Standards (CFATS)-covered facilities. CAVs are designed to provide in-depth knowledge of and assistance to comply with CFATS. For more information, see www.dhs.gov/files/programs/gc_1247235870769.shtm or contact cfats@hq.dhs.gov.

Chemical Security Summit The Cybersecurity and Infrastructure Security Agency's Chemical 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 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 CISA Chemical SSA at chemicalsector@hq.dhs.gov.

Chemical Sector Classified Briefing The Chemical Sector Specific Agency 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 www.fema.gov/technological-hazards/chemical-stockpile-emergency-preparedness-program.

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 Cybersecurity and Infrastructure Security Agency Chemical Sector Specific Agency 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 Cybersecurity and Infrastructure Security Agency Chemical Sector Specific Agency 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 Cybersecurity and Infrastructure Security Agency 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 www.dhs.gov/files/programs/gc_1181835547413.shtm. For more information, contact the CFATS Help Desk at csat@dhs.gov 866-323-2957.

Critical Infrastructure Tabletop Exercise Program (CITEP) Chemical Sector Tabletop Exercise (TTX) The CITEP 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 Cybersecurity and Infrastructure Security Agency Chemical Sector Specific Agency 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 Sector Specific Agency 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 the Homeland Security Information Network 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 Sector Specific Agency 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 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 Chemical Sector Specific Agency 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 Chemical Sector Specific Agency 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 Chemical Sector Specific Agency at chemicalsector@hq.dhs.gov.

Critical Infrastructure – Multiple Sectors

Critical Infrastructure Learning Series The

Learning Series allows the Cybersecurity and Infrastructure Security Agency 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 www.dhs.gov/ciwebinars.

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 the 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: https://training.fema.gov/is/courseoverview.aspx?code=is-860.c.

DHS Center of Excellence: Critical Infrastructure Resilience Institute (CIRI), led by the University of Illinois Urbana-Champaign, conducts research and education to enhance the resiliency of the nation's critical infrastructures and the businesses and public entities that own and operate those assets and systems. The Institute explores the organizational, policy, business, and technical dimensions of critical infrastructure's dependence on cyber assets. CIRI also examines how computer hardware and software both contribute to and threaten resiliency and how industry makes decisions about cyber assets which contribute to resilience. For more information, see www.ciri.illinois.edu. For more information, contact universityprograms@hq.dhs.gov.

Critical Infrastructure Training Module provides an overview of the National Infrastructure Protection Plan 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 Sector Outreach and Programs Division (SOPD) sectors and generally contain sector overviews; information on sector partnerships; information on critical infrastructure protection issues and priority programs. For more information, see www.dhs.gov/xlibrary/assets/nipp_annrpt.pdf. For more information, contact nipp@dhs.gov.

Active Shooter Security Preparedness 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, and 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 Cybersecurity and Infrastructure Security Agency 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 CISA has developed the Dealing with Workplace Violence 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 if 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 CISA Sector Outreach and Programs Division at sopdexecsec@hq.dhs.gov.

Enduring Security Framework (ESF) The ESF is a cross-sector working group comprised of public and private sectors taking collaborative steps to proactively mitigate risks and strengthen cybersecurity posture in efforts to obtain a

secure and resilient cyberspace. For more information, visit https://www.dhs.gov/publication/cipac-cs-esf-agendas# or contact esf@hq.dhs.gov.

FoodSHIELD is a Web-based system for communication, coordination, community-building, education, and training among the nation's food and agriculture sectors. Developed by the Food Protection and Defense Institute (FPDI), a DHS Emeritus Center of Excellence, 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 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, https://foodprotection.umn.edu/ or email universityprograms@hq.dhs.gov.

DHS Center of Excellence: Global Terrorism Database (GTD) 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 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 dependent on the level of customization and the mode of delivery. For more information, see www.start.umd.edu or universityprograms@hq.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 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 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@hq.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 nep@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 www.fema.gov/nonprofit-security-grant-program or contact the FEMA Centralized Scheduling and Information Desk at askcsid@fema.dhs.gov or 1-800-368-6498.

Cybersecurity and Infrastructure Security Agency 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 www.dhs.gov/files/programs/gc_1189168948944.shtm.

Cybersecurity and Infrastructure Security Agency 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: www.dhs.gov/files/training/training-critical-infrastructure-partners.shtm.

Protective Security Advisors (PSAs) are Cybersecurity and Infrastructure Security Agency 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 critical infrastructure assets and DHS. For more information, see www.dhs.gov/cisa/protective-security-advisors.

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 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@hq.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.

Cybersecurity Infrastructure Security Agency /Transportation Security Administration 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 TSA's Intermodal Security Training and Exercise Program (ISTEP). For more information, please contact CISA Critical Manufacturing Sector Specific Agency at criticalmanufacturing@hq.dhs.gov.

Insider Threat Programs for the Critical Manufacturing Sector Implementation Guide The Insider Threat Programs for the Critical Manufacturing Sector Implementation Guide was developed to provide guidance and information for critical manufacturing organizations to establish insider threat programs. These programs serve to gather, monitor, and assess information for insider threat detection and mitigation strategies. Insider threat programs are designed to detect, deter, and mitigate the risks associated with trusted insiders and protect the privacy of the workforce while reducing potential harm to the organization. Effective insider threat programs deploy risk management strategies that identify the assets or resources to be protected, identify potential threats, determine vulnerabilities, assess risk, and deploy countermeasures. For more information, email 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-page/fact sheet. For more information, please contact the CISA Commercial Facilities Sector Specific Agency at cfsteam@hq.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 CISA Commercial Facilities SSA at cfsteam@hq.dhs.gov.

DHS Retail Video: "What's in Store—Ordinary People/Extraordinary Events" CISA 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

act when suspicious behavior is identified. The video can be viewed at www.dhs.gov/video/whats-store-ordinary-people-extraordinary-events. For more information, please contact the CISA Commercial Facilities Sector Specific Agency at cfsteam@hq.dhs.gov.

Partners in Prevention: *Vehicle Rentals and Vehicle Ramming Video* DHS CISA and TSA, and the Federal Bureau of Investigation—in coordination with the Truck Renting and Leasing Association and the American Car Rental Association—have released a short training video to help vehicle rental employees identify suspicious activities and behavior by customers who may wish to use a rented vehicle for nefarious purposes. The video can be viewed at: www.fbi.gov/video-repository/vehicle-rentals-vehicle-ramming-013019.mp4/view. For more information, please contact the CISA Commercial Facilities Sector Specific Agency at cfsteam@hq.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 Cybersecurity and Infrastructure Security Agency Commercial Facilities Sector Specific Agency at cfsteam@hq.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 Sector Coordinating Council and the Lodging Subsector and is available at www.dhs.gov/xlibrary/assets/ip_cikr_hotel_advisory.pdf. For more information, please contact the Cybersecurity and Infrastructure Security Agency Commercial Facilities Sector Specific Agency at cfsteam@hq.dhs.gov.

Critical Infrastructure Tabletop Exercise Program 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 CITEPs 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 Cybersecurity and Infrastructure Security Agency Commercial Facilities Sector Specific Agency at cfsteam@hq.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: https://training.fema.gov/is/courseoverview.aspx?code=IS-906. For more information about Office of Infrastructure Protection training courses, please contact independent.study@fema.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: https://training.fema.gov/is/courseoverview.aspx?code=IS-907. For more information about Office of Infrastructure Protection training courses, please contact: independent.study@fema.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: https://training.fema.gov/is/courseoverview.aspx?code=IS-912. For more information about Office of Infrastructure Protection training courses, please contact: independent.study@fema.dhs.gov.

Lodging Video: "No Reservations: Suspicious Behavior in Hotels" 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 Cybersecurity and Infrastructure Security Agency Commercial Facilities Sector Specific Agency 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 Cybersecurity and Infrastructure Security Agency Commercial Facilities Sector Specific Agency at cfsteam@hq.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 Cybersecurity and Infrastructure Security Agency 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 Cybersecurity and Infrastructure Security Agency 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 Cybersecurity and Infrastructure Security Agency Commercial Facilities Sector Specific Agency at cfsteam@hq.dhs.gov.

Public Venue Bag Search Procedures Guide This guide provides suggestions for developing and implementing bag search procedures at public assembly venues hosting a variety of events, which may include sporting events, concerts, family festivals, or other public gatherings. Venue owners, operators, and event organizers may also choose to use additional resources (e.g., consult law enforcement) to supplement the procedures outlined in this guide.

Bag search procedures are meant to control items that are hand-carried into a venue and may be a part of a venue's overall security plan. This document provides guidance on how to:

- Prepare and plan for bag search procedures in advance of an event;
- Deter individuals from bringing illegal, prohibited, or unusual items into the venue;
- Interact with individuals who are having their bag(s) searched;
- Conduct a bag search and identify items of interest (i.e., illegal, prohibited, or unusual); and
- Respond when items of interest are discovered during a bag search.

The bag search procedures outlined in this document are for guidance purposes only; they are not required under any regulation or legislation. In addition, due to the wide variation in the types, sizes, and locations of public assembly venues and the types of events held in these venues, not all suggested procedures will be relevant or applicable. The guide is available here: www.dhs.gov/sites/default/files/publications/public_venue_bag_search_procedures_guide_3jun2019_v2_final_508.pdf. For more information, contact the Cybers1ecurity and Infrastructure Security Agency Commercial Facilities Sector Specific Agency at cfsteam@hq.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 Cybersecurity and Infrastructure Security Agency Commercial Facilities Sector Specific Agency at cfsteam@hq.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 Homeland Security Information Network – Critical Sectors Commercial Facilities portal at https://connect.hsin.gov/p21849699/. For more information, contact the Commercial Facilities Sector Specific Agency at cfsteam@hq.dhs.gov.

Communications Sector

Network Security Information Exchange (NSIE) The National Security Telecommunications Advisory Committee recommended the establishment of an Industry- partnership to reduce the vulnerability of the Nations' telecommunications systems to electronic intrusion. The NSTAC formed separate government and industry NSIEs to share ideas on technologies and techniques for addressing and mitigating the risks to the public network and its supporting infrastructures. For more information, visit www.dhs.gov/publication/nsie-fact-sheet or contact nsie@hq.dhs.gov.

National Security Telecommunications Advisory Committee Recommendations address national security and emergency preparedness issues from a private sector perspective and reflect over a quarter-century of private sector advice to the president and the nation. Issues include network convergence, network security, emergency communications operations, resiliency and emergency communications interoperability. NSTAC recommendations can be found at www.dhs.gov/cisa/national-security-telecommunications-advisory-committee. For more information, contact nstac@hq.dhs.gov.

Dams Security

Active and Passive Vehicle Barriers Guide (Dams Sector) 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 CISA Dams Sector Specific Agency at dams@hq.dhs.gov.

The **Consequence-Based Top Screen (CTS) Fact Sheet** provides information pertaining to the CTS methodology, including how it was developed, its primary purpose, and the Web-based tool with which it is implemented. For more information, see www.dhs.gov/files/programs/gc_1260541882284.shtm or contact the CISA Dams Sector Specific Agency at dams@hq.dhs.gov.

Dams and Energy Sector Interdependency Study focuses on the importance of hydroelectric power generation and the major risk factors that affect

the ability of hydropower facilities to produce the electricity they need at the right time. For more information, please contact the Cybersecurity and Infrastructure Security Agency Dams Sector Specific Agency at dams@hq.dhs.gov.

Dams Sector Consequence-Based Top Screen Reference Guide provides information on the CTS methodology, how it was developed, its primary purpose, and the web-based tool with which it is implemented. For more information, please contact the Cybersecurity and Infrastructure Security Agency Dams Sector Specific Agency at dams@hq.dhs.gov.

Dams Sector Crisis Management Handbook provides an introduction to crisis management measures for dam owners. It explains how such measures are an important component of an overall risk management program. In addition, it describes major components of crisis management and provides a template and guidelines that might be useful in developing these components for other dams. For more information, please contact the Cybersecurity and Infrastructure Security Agency Dams Sector Specific Agency at dams@hq.dhs.gov.

Roadmap to Secure Control Systems in the Dams Sector describes a plan or roadmap and strategic vision for voluntarily improving the cybersecurity posture of control systems within the Dams Sector. Designing, operating, and maintaining a facility to meet essential reliability, safety, and security needs requires careful evaluation and analysis of physical, cyber, and human risk factors. The interaction of both internal and external process and business systems must also be considered. A cyber event, whether caused by an external adversary, an insider threat, or inadequate policies and procedures, can initiate a loss of system control resulting in negative consequences. This roadmap recognizes this interconnectivity but restricts its scope by addressing the cyber issues of control systems. It highlights recommended strategies to address sector challenges, specifies mitigation requirements, and lists long-term research and development needs regarding control system security. For more information, please contact the Cybersecurity and Infrastructure Security Agency Dams Sector Specific Agency at dams@hq.dhs.gov.

The **Surveillance and Suspicious Activity Indicators Guide for Dams and Levees** provides members of the Dams Sector with the capability to report and retrieve information pertaining to suspicious activities that may potentially be associated with pre-incident surveillance, activities exploring or targeting a critical infrastructure facility or system, or any possible violation of law or regulation that could compromise the facility or system in a manner that could cause an incident jeopardizing life or property. For more information, please contact the Cybersecurity and Infrastructure Security Agency Dams Sector Specific Agency at dams@hq.dhs.gov.

Dams Sector Suspicious Activity Reporting Fact Sheet provides information regarding the online Suspicious Activity Reporting tool within the Homeland Security Information Network – Critical Infrastructure 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 Cybersecurity and Infrastructure Security Agency Dams Sector Specific Agency at dams@hq.dhs.gov.

Dams Sector Tabletop Exercise Toolbox (DSTET) provides dam owners and operators with exercise planning resources to address sector-specific threats, issues, and concerns related to the protection of dams. DSTET allows exercise participants to address key issues through a series of facilitated discussions. The intent of the toolbox is to enhance effective information sharing and coordination between owners and operators, first responders, and relevant stakeholders during various threat and incident phases as detailed in the corresponding scenarios. For more information, please contact the Cybersecurity and Infrastructure Security Agency Dams Sector Specific Agency at dams@hq.dhs.gov.

Dams Sector Waterside Barriers Guide was developed to assist dam owners and operators in understanding the possible need for waterside barriers as part of their overall security plan. It provides owners, operators, and security personnel with a very cursory level of information on barriers and their use, maintenance, and effectiveness—elements that must be carefully considered when selecting waterside barriers. For more information, please contact the Cybersecurity and Infrastructure Security Agency Dams Sector Specific Agency at dams@hq.dhs.gov.

Dams Sector Web-Based Training Courses 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 Cybersecurity and Infrastructure Security Agency Dams Sector Specific Agency 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 Sector Specific Agency at dams@hq.dhs.gov.

Dams Sector 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 Cybersecurity and Infrastructure Security Agency Dams Sector Specific Agency at dams@hq.dhs.gov.

Dams Sector 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 Cybersecurity and Infrastructure Security Agency Dams Sector Specific Agency at dams@hq.dhs.gov.

IS-870 Dams Sector: Crisis Management Overview This online training course addresses crisis management activities as an important component of an overall risk management program, and provides dam and levee stakeholders with recommendations to assist in the development of various plans focused on enhancing preparedness, protection, recovery, and resilience capabilities. The training course describes the purpose and basic elements of emergency action plans, recovery plans, and continuity plans; and addresses the basic elements of an effective exercise program. For more information, please contact the Cybersecurity and Infrastructure Security Agency Dams Sector Specific Agency 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. An effective screening protocol for potential employees and contractor support can contribute to enhanced facility security by ensuring that untrustworthy individuals do not gain employment or access to sensitive facilities or information. For more information, please contact Cybersecurity and Infrastructure Security Agency Dams Sector Specific Agency 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. For more information please contact the Cybersecurity and Infrastructure Security Agency Dams Sector Specific Agency at dams@hq.dhs.gov.

Dams Sector Suspicious Activity Reporting Fact Sheet provides information regarding the online Suspicious Activity Reporting tool within the Homeland Security Information Network – Critical Infrastructure 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 Cybersecurity and Infrastructure Security Agency Dams Sector Specific Agency 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 Infrastructure(HSIN-CI). The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) is a joint collaborative effort by the U.S. Department of Homeland Security, the Federal Bureau of Investigation, and state, local, tribal, and territorial law enforcement partners. This initiative provides law enforcement with another tool to help prevent terrorism and other related criminal activity by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information. For more information visit https://www.dhs.gov/nsi.

Security and Protection of Dams and Levees Workshop (L260) provides dam owners and operators, emergency managers, and other relevant stakeholders with information on the

fundamental aspects of security and protection for dams, levees, and related facilities. For more information, contact the Cybersecurity and Infrastructure Security Agency Dams Sector Specific Agency at dams@hq.dhs.gov.

Dams Sector Security Guidelines consolidate effective industry security practices into a framework to help owners and operators select and implement security activities and measures that reduce risk; improve the protection of personnel, public health, and public safety; and reinforce public confidence. For more information, contact the Dams Sector Specific Agency at dams@hq.dhs.gov.

Dams Sector Cybersecurity Capability Maturity Model (C2M2) aims to advance the practice of cybersecurity risk management across the Dams Sector by providing all Dams Sector organizations, regardless of size or type, with a flexible tool to help them evaluate, prioritize, and improve their cybersecurity capabilities. For more information, contact the Cybersecurity and Infrastructure Security Agency Dams Sector Specific Agency at dams@hq.dhs.gov.

Dams Sector Cybersecurity Capability Maturity Model (C2M2) Implementation Guide is a supplement to the C2M2. The guidance provided in this publication is intended to address the implementation and management of cybersecurity practices associated with information technology and operations technology assets and the environments in which they operate. For more information, contact the Cybersecurity and Infrastructure Security Agency Dams Sector Specific Agency at dams@hq.dhs.gov.

Dams Sector Cybersecurity Framework Implementation Guidance enables an organization-regardless of its size, degree of risk, or cybersecurity sophistication-to apply the principles and effective practices of cyber risk management to improve the security and resilience of its critical infrastructure. For more information, contact the Cybersecurity and Infrastructure Security Agency Dams Sector Specific Agency at dams@hq.dhs.gov.

Dams Sector Cybersecurity Program Guidance outlines various strategies and methods to develop or improve a basic cybersecurity program, enabling dam owners and operators to select cybersecurity activities and measures appropriate to their cyber assets and risk profiles. For more information, contact the Cybersecurity and Infrastructure Security Agency Dams Sector Specific Agency at dams@hq.dhs.gov.

Food Safety and Influenza

DHS Emeritus Center of Excellence: Center for Zoonotic and Animal Disease Defense (ZADD), a co-led Center of Excellence between the Institute of Infectious Animal Diseases (IIAD) at Texas A&M University and the Center of Excellence for Emerging and Zoonotic Animal Diseases (CEEZAD) at Kansas State University. The DHS Emeritus Center develops innovative solutions and fosters collaborations to protect the nation's agriculture and public health sectors against high-consequence foreign animal, emerging, and zoonotic disease threats. The research and education capabilities include, next-generation vaccine candidate development, decision support systems and emergency management tools for animal disease threats, animal agriculture systems analyses, and education and training for the current and future homeland security workforce. For more information see, iiad.tamu.edu for IIAD and ceezad.org for CEEZAD, or contact universityprograms@hq.dhs.gov.

DHS Emeritus Center of Excellence: Food Protection and Defense Institute (FPDI), led by the University of Minnesota, is a multidisciplinary, action-oriented research consortium united to help make the nation's food system less vulnerable to a biological or chemical attack. Through research and education, FPDI looks to safeguard the food system comprehensively, from farm to table, to reduce the potential for contamination at any point along the food supply chain and a catastrophic attack on public health and the economy. For more information, see http://foodprotection.umn.edu/ or contact universityprograms@hq.dhs.gov.

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

Sector-Specific Pandemic Influenza Guides The Cybersecurity and Infrastructure Security

Agency developed sector-specific guides for pandemic influenza for the Chemical, Commercial Facilities, Dams, Emergency Services, and Nuclear Sectors. For more information, please contact the Sector Outreach and Programs Division at SOPDExecSec@hq.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 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 www.tsa.gov/stakeholders/trucking-hazmat or contact TSA Highway and Motor Carrier Division at highwaysecurity@dhs.gov.

Hazmat Motor Carrier Security Self-Assessment Training Program addresses the requirements contained in 49 Code of Federal Regulations, 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 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 1 HSSM and Tier 2 HSSM. The security practices are voluntary to allow highway motor carriers to adopt measures best suited to their circumstances. For more information, see http://www.tsa.gov/stakeholders/trucking-hazmat or contact highwaysecurity@dhs.gov.

Hazardous Materials Endorsement Threat Assessment Program The Hazardous Materials Endorsement Threat Assessment Program conducts a threat assessment for any driver seeking to obtain, renew and transfer a hazardous materials endorsement on a state-issued commercial driver's license. For more information, visit www.tsa.gov/for-industry/hazmat-endorsement

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 www.phmsa.dot.gov/hazmat/risk/rmsef or contact highwaysecurity@dhs.gov.

Infrastructure Security and Resilience Assessment

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 www.tsa.gov/stakeholders/advancing-security-baseline or contact masstransitsecurity@dhs.gov.

The Risk Management Process: An Interagency Security Committee Standard This standard

defines the criteria and processes that those responsible for a facility's security should use in determining its security level. This standard provides an integrated, single source of physical security countermeasures and guidance on countermeasure customization for all non-military federal facilities. For more information, please see www.dhs.gov/files/committees/gc_1194978268031.shtm.

Assist Visits are conducted by PSAs in collaboration with critical infrastructure owners and operators to assess overall facility security and increase security awareness. Assist Visits are augmented by either the Security Assessment on First Entry (SAFE) or the Infrastructure Survey Tool (IST). The SAFE tool is designed to assess the current security posture and identify options for facility owners and operators to mitigate relevant threats. It is not intended to be an in-depth security assessment. A SAFE may be the first step toward an effective security program. It is generally intended for facilities that have little or no security measures or planning in place. The IST is a web-based tool that provides the ability to collect, process, and analyze Assist Visit survey data in real time. Data collected during an Assist Visit is consolidated in the IST and then weighted and valued, which enables DHS to develop 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 Assist Visit should contact isdassessments@hq.dhs.gov.

The **Infrastructure Survey Tool (IST)** is a voluntary, web-based security survey conducted by PSAs in coordination with facility owners and operators after an Assist Visit to identify and document the overall security and resilience of the facility. The security survey is conducted to: identify facilities' physical security, security forces, security management, information sharing, protective measures, and dependencies related to preparedness, mitigation, response, resilience, and recovery; identify security gaps; create facility protective and resilience measures indices that can be compared to similar facilities; and track progress toward improving critical infrastructure security. If you would like to learn more about ISTs, please contact isdassessments@hq.dhs.gov.

Regional Resiliency Assessment Program (RRAP) is a cooperative assessment of specific critical infrastructure within a designated geographic area and a regional analysis of the surrounding infrastructure that address a range of infrastructure resilience issues that could have regionally and nationally significant consequences. These voluntary, non-regulatory RRAP projects are led by the Infrastructure Security Division, within the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency and are selected each year by the Department with input and guidance from federal, state, and local partners. The goal of the RRAP is to generate greater understanding and action among public and private sector partners to improve the resilience of a region's critical infrastructure. Private sector owners and operators interested in receiving more information on the RRAP should contact isdassessments@hq.dhs.gov.

Critical Infrastructure Tabletop Exercise Program, formerly known as Sector-Specific Tabletop Exercise Program (SSTEP), is designed to assist critical infrastructure owners and operators in developing their own tabletop exercises to meet the specific needs of their facilities and stakeholders. The CITEP allows users to leverage pre-built exercise templates and vetted scenarios to build tabletop exercises to assess, develop, and update information sharing processes, emergency plans, programs, policies, and procedures. This program provides exercise planners with tools, scenarios, question sets, and guidance in developing an interactive discussion-based exercise for their communities of interest (COI). Each CITEP template can be customized and further developed to exercise and evaluate specific areas of concern for critical infrastructure owners and operators. The CITEP fosters effective partnership building through the development of improved information sharing and collaboration. In addition, the CITEP enables the development of after-action reports that support mitigating risks while increasing the resilience of critical infrastructure. Currently there are over 50 scenarios, both natural hazards and human threats, that users can modify to meet their organization's needs. For more information, please contact the Infrastructure Stakeholder Security and Exercise Program at issep@hq.dhs.gov.

Infrastructure Stakeholder Security Exercise Program Well-designed and well-executed exercises are the most effective means of assessing and validating policies, plans, procedures, training, equipment, assumptions,

and inter-organizational agreements. Exercises are vital for clarifying roles and responsibilities, as well as improving coordination and communication. As well as identifying gaps in resources, exercises will measure performance and identify opportunities for improvement, increasing the ability for critical infrastructure stakeholders to mitigate, respond to, and recover from threat-based incidents. The Infrastructure Stakeholder Security Exercise Program (ISSEP) exercise team designs, develops, and executes both discussion-based and operations-based exercises on behalf of Infrastructure Security Division critical infrastructure community partners throughout the nation. The ISSEP exercise team conducts exercises to support preparedness and resilience priorities specifically related to critical infrastructure and soft targets and assists stakeholders in identifying opportunities to tailor their information sharing, response and recovery procedures into decisive and actionable plans through the after-action reporting process. For more information please contact the Cybersecurity and Infrastructure Security Agency Infrastructure Stakeholder Security and Exercise Program at issep@hq.dhs.gov.

Land Transportation and Pipeline

Countering Improvised Explosive Devices Training for Pipeline Employees is a DVD-based training program to familiarize pipeline company employees and contractors with the threat posed by 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 www.crti.uconn.edu/ or contact universityprograms@hq.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: www.firstobserver.com/training/home.php or contact firstobserver@hms-world.com or 888-217-5902.

Highway and Motor Carrier Awareness Posters include Motor coach 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 www.tsa.gov/stakeholders/trucking-hazmat or contact highwaysecurity@dhs.gov.

Highway Information Sharing and Analysis Center (ISAC) The TSA Trucking Security Program funds the First Observer ™ domain awareness program as well as a Call-Center and ISAC. The Highway ISAC creates products and bulletins and emails 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 or call 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 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 www.tsa.gov/stakeholders/documents-and-reports-0 or contact highwaysecurity@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 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 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 www.tsa.gov/stakeholders/pipeline-security.

Safeguarding America's Transportation System Security Guides are available for highway passenger security motor coach 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 www.tsa.gov/stakeholders/school-transportation-security-awareness or contact highwaysecurity@dhs.gov.

Transportation Sector Network Management Highway and Motor Carrier Division Annual Report TSA Highway and Motor Carrier Division publishes an annual report and posts the document on the following website 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, motor coach, 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, and 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 to 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 Harbor Safety Committees (HSC) 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 Area Maritime Security Committees (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 www.uscg.mil/hq/cg5/cg544/amsc.asp, 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 U.S. 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.

AMSPs are exercised annually through the **U.S.** 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 U.S. Coast Guard Journal of Safety at Sea is the voice of the U.S. 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: Arctic Domain Awareness Center (ADAC) led by the University of Alaska – Anchorage, develops and transitions technology solutions, innovative products, and educational programs to improve situational awareness and crisis response capabilities related to emerging maritime challenges posed by the dynamic Arctic environment. For more information, see http://arcticdomainawarenesscenter.org/ or contact universityprograms@hq.dhs.gov.

DHS Center of Excellence: Coastal Resilience Center (CRC), led by the University of North Carolina at Chapel Hill in partnership with Jackson State University in Mississippi, conducts research and education to enhance the nation's ability to safeguard people, infrastructure, and economies from catastrophic coastal natural disasters such as floods and hurricanes. Resources include the ADCIRC Prediction System for storm surge and coastal flooding and the Plan Integration for Resilience Scorecard (PIRS) for community hazard vulnerability reduction. For more information, visit https://coastalresiliencecenter.unc.edu/ or contact universityprograms@hq.dhs.gov.

DHS Center of Excellence: Maritime Security Center (MSC), led by Stevens Institute of Technology, enhances maritime domain awareness and develops strategies to support marine transportation system resilience and educational programs for current and aspiring homeland security practitioners. For more information, see www.stevens.edu/research-entrepreneurship/research-centers-labs/maritime-security-center or contact universityprograms@hq.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 see www.harborsafetycommittee.blogspot.com.

HOMEPORT is the primary on-line means of communicating alerts, announcements and other information from the U.S. 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 call 571-227-3556.

Maritime Security Risk Analysis Model is a terrorism risk management tool and process used to conduct scenario-based risk assessments against critical infrastructure, key assets, and targets within each U.S. Coast Guard Captains of the Port area of responsibility. The execution of the MSRAM process is built upon the

assessments and judgments made by U.S. 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 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 U.S. Customs and Border Protection requirements. For more information, see 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 U.S. 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 (PSGP) provides funds for transportation infrastructure security activities to implement Area Maritime Security Plans and facility security plans among port authorities, facility operators, and state and local government agencies required to provide port security services. For more information, see https://www.fema.gov/port-security-grant-program or contact the FEMA Centralized Scheduling and Information Desk at askcsid@fema.dhs.gov or 1-800-368-6498.

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 U.S. 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 only authorized individuals who complete a TSA Security Threat Assessment and do not pose a national or transportation security threat may gain unescorted access to secure areas of the Nation's maritime transportation system. On successful completion of the assessment, TSA issues a biometric security card, termed the TWIC® card, which permits maritime facilities and vessels to grant the cardholder unescorted access to U.S. Coast Guard-regulated secure areas. Most mariners licensed by the U.S. Coast Guard also require a credential. The TWIC® is valid for five-years from date of issuance, and all TWIC® cardholders are subject to recurrent vetting for potential disqualifying factors. For more information, see www.tsa.gov/for-industry/twic or contact 855-347-8371. For general TWIC® issues, please contact twic.issue@tsa.dhs.gov.

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 U.S. 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 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 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 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 www.uscg.mil/hq/cg5/nvdc/ for more information or call 800-799-8362 or 304-271-2400 (7:30 a.m. to 5:00 p.m. Eastern Time).

Mass Transit and Rail Security

The **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 Bus Security Grant Program (IBSGP) provides funds to owners and operators of intercity bus systems to protect critical surface transportation infrastructure and the traveling public from acts of terrorism and to increase the resilience of transit infrastructure. For more information, see www.fema.gov/intercity-bus-security-grant-program or contact the FEMA Centralized Scheduling and Information Desk at askcsid@fema.dhs.gov or 1-800-368-6498.

Intercity Passenger Rail (IPR) Program provides funding to the National Railroad Passenger Corporation (Amtrak) to protect critical surface transportation infrastructure and the traveling public from acts of terrorism and to increase the resilience of the Amtrak rail system. For more information, see /www.fema.gov/intercity-passenger-rail-amtrak or contact the FEMA Centralized Scheduling and Information Desk at askcsid@fema.dhs.gov or 1-800-368-6498.

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.

The **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 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 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 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 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.

Transit Security Grant Program provides funds to owners and operators of transit systems (which include intra-city bus, commuter bus, ferries, and all forms of passenger rail) to protect and increase the resilience of critical surface transportation infrastructure and the traveling public from acts of terrorism. For more information, see www.fema.gov/transit-security-grant-program or contact the FEMA Centralized Scheduling and Information Desk at askcsid@fema.dhs.gov or 1-800-368-6498.

Nuclear Security

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. NNFEDP promotes a unique interdisciplinary approach that encourages collaboration among academic programs, universities, and DOE's 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, www.dhs.gov/blog/2012/08/28/supporting-next-generation-nuclear-forensic-scientists, or contact cwmdcomms@hq.dhs.gov.

Nuclear Sector Classified Threat Briefing The Cybersecurity and Infrastructure Security Agency Nuclear Sector Specific Agency coordinates both regularly scheduled and incident-specific classified briefings for cleared sector partners. For more information, please contact the Nuclear SSA at nuclearssa@hq.dhs.gov.

Nuclear Sector Information Sharing Standard Operating Procedure (SOP) is designed to enhance the effectiveness of voluntary

information coordination and distribution among members of the Nuclear Sector Information Sharing Environment. 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 Nuclear Sector Specific Agency 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.

Radiological Emergency Preparedness Program (REP) coordinates the national effort to provide state, local, and tribal governments with relevant and executable planning, training, and exercise guidance and policies necessary to ensure that adequate capabilities exist to prevent, protect against, mitigate the effects of, respond to, and recover from incidents involving commercial nuclear power plants (NPPs). For more information, visit: www.fema.gov/radiological-emergency-preparedness-program.

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 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.

DHS Emeritus Center of Excellence: National Center for Visualization and Data Analytics (CVADA), co-led by Purdue University and Rutgers University, 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 information and related technologies. 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 www.purdue.edu/discoverypark/vaccine/ and www.ccicada.org/ or contact universityprograms@hq.dhs.gov.

DHS Emeritus Center of Excellence: National Consortium for the Study of Terrorism and Responses to Terrorism, led by the University of Maryland, 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 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 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.

DHS National Operations Center (NOC) Common Operating Picture (COP) is a secure, web-based geospatial information systems portal that provides situational awareness and decision support to homeland security partners at all levels of government. The DHS NOC COP integrates and fuses 800+ data layers and partner IT systems and databases into a one-stop-shop clearinghouse for information regarding acute, emergent incidents/events.

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 or private sector partners may request that they be added to distribution by emailing 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. Developed by the Food Protection and Defense Institute, a DHS Emeritus Center of Excellence, FASCAT is used 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 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*. 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 at 1-866-430-0162 or 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, 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.

Homeland Security Information Network-Federal Operations (HSIN FedOps) is the primary information sharing platform for homeland security partners regarding acute, emergent incidents, events, and threats affecting the homeland. HSIN FedOps enables mission partners at all levels of government to coordinate and share incident, events, and threat information in near-real time. For access to HSIN FedOps, contact the National Operations Center HSIN Desk Officer at noc.hsin@hq.dhs.gov. When requesting access, please provide name, agency/organization, supervisor's name/e-mail/phone number, and your official e-mail address and phone number.

"If You See Something, Say Something®" Campaign In July 2010, the Department of Homeland Security (DHS) launched the national "If You See Something, Say Something®" campaign that raises public awareness of the indicators of terrorism and terrorism-related crime, as well as the importance of reporting suspicious activity to state and local law

enforcement. The campaign was originally implemented and trademarked by the New York Metropolitan Transportation Authority and is licensed to DHS for creating a nationwide campaign. For more information, visit www.dhs.gov/see-something-say-something.

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 can 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. 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 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 group, and then apply additional, associated taxonomy levels to detail the specifics of the asset and describe its functions. For more information, see www.dhs.gov/files/publications/gc_1226595934574.shtm or visit https://taxonomy.iac.anl.gov/ to use the tool or contact: idt@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.

I&A Private Sector Engagement Corporate Security Symposia (CSS) The CSS are a series of regional day-long conferences held around the country focused on topics critical to national security. They feature prominent speakers from both the public and private sectors who shed light on how to best leverage corporate security efforts and analytic capabilities to address issues such as terrorism, insider threat, cyber security, critical infrastructure protection, and other national security challenges. Each symposium draws 200-400 private sector and other homeland security professionals. For more information, including upcoming CSS dates, see www.dhs.gov/private-sector-engagement.

I&A Private Sector Engagement Public-Private Analytic Exchange Program (AEP)
The AEP enables government and private sector analysts to gain a greater understanding of how their distinct missions can benefit from public-private collaboration on topics of mutual interest. Each year, public and private sector subject matter experts work together on virtual teams to develop unclassified analytic deliverables reflecting emerging and high visibility topics related to homeland security over the course of six months. These deliverables are broadly disseminated at the unclassified level to all stakeholders. For more information, including deliverables created through the AEP, see www.dhs.gov/private-sector-engagement.

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 classroom and online. 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 www.biometrics.gov/nstc/default.aspx or contact info@biometrics.org.

National Science and Technology Council (NSTC) Subcommittee on Open Science (SoS) oversees all agencies efforts to improve the public's access to the results of federally funded research; specifically, peer-reviewed scholarly publications and digital data. DHS has established a repository through PubMed Central (PMC), developed and maintained by the National Institutes of Health (NIH)/National Library of Medicine (NLM) for approved peer-reviewed journal articles and other releasable manuscripts. A separate cloud-based repository has been established through a commercial provider for ready access to digitally formatted scientific datasets associated with the journal articles and other scholarly works. For more information, see www.ncbi.nlm.nih.gov/pmc/funder/dhs or contact kmo@hq.dhs.gov.

The Nationwide Suspicious Activity Reporting Initiative 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.

The National Threat Assessment Center (NTAC) is a component of the U.S. Secret Service that conducts research, training, consultation, and information sharing on threat assessment and the prevention of targeted violence. NTAC's work is based on its original research into attacks directed at government officials and agencies, workplaces, K-12 schools, colleges and universities, and mass attacks in public spaces, which served as the building blocks for the Secret Service's threat assessment model. All NTAC's reports are made available to government agencies, law enforcement, schools, and private sector partners. Recent products include the annual reports on mass attacks in public spaces (released July 2019) and an operational guide to establishing threat assessment capabilities at K-12 school that offers actionable steps to Enhancing School Safety Using a Threat Assessment Model (released July 2019). All NTAC publications are available at www.secretservice.gov/protection/ntac/.

Protected Critical Infrastructure Information (PCII) Program was created by Congress under the Critical Infrastructure Information (IIC) Act of 2002 and implemented in federal regulation under 6 CFR part 29. The program protects CII voluntarily submitted by private sector or state, local, tribal and territorial owner operators to the federal government from disclosure under the Freedom of Information Act, state/local disclosure laws, civil litigation, and regulatory use. To qualify for PCII protections, information must be voluntarily submitted, not customarily found in the public domain, and not submitted in lieu of compliance with any regulatory requirement. Information about the PCII Program can be found at www.dhs.gov/pcii. For additional information, contact pcii-assist@hq.dhs.gov or the PCII Help Desk at 866-844-8163.

Sensitive Security Information Program Sensitive Security Information (SSI) is information obtained or developed which, if released publicly, would be detrimental to transportation security, and is defined at 49 CFR Part 1520. SSI is not authorized for public disclosure and is subject to handling and safeguarding restrictions. The TSA SSI

Program, the central SSI authority for all of DHS, develops SSI guidance and training materials to assist transportation security partners in the recognition and safeguarding of SSI. The SSI Program also develops SSI policies and procedures, analyzes and reviews records for SSI content, and coordinates with stakeholders, other government agencies and Congress on SSI-related issues. For more information about SSI or for assistance in identifying SSI, visit www.tsa.gov/for-industry/sensitive-security-information or contact ssi@hq.dhs.gov.

Cybersecurity and Infrastructure Security Agency Classified Threat Briefings CISA coordinates both regularly scheduled and incident-specific classified briefings for cleared sector partners. For more information, contact the CISA Sector Outreach & Programs Division at sopdexecsec@hq.dhs.gov.

Surveillance Detection Awareness on the Job is a 90-minute interactive web presentation designed to raise awareness of suspicious behaviors that might indicate potential surveillance activities. This virtual production offers cross-sector examples of suspicious activities and behaviors and provides information to help identify and report such behaviors in a timely manner. The webinar features a moderated roundtable discussion of five diverse examples of surveillance and detection, as well as information about the resources available for timely reporting of suspicious activities. The live webinar is available for download on 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 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 the Cybersecurity and Infrastructure Security Agency Office for Bombing Prevention at obp@hq.dhs.gov or view 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 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 Cybersecurity and Infrastructure Security Agency Commercial Facilities Sector Specific Agency at cfsteam@hq.dhs.gov.

TSA Alert System is an emergency notification alert system for highway and motor carrier security partners. The system can send a message via phone, email 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 ongoing 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 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/.

and Insider Threat Mitigation

Soft Targets and Crowded Places (ST-CPs), such as sports venues, shopping venues, schools, and transportation systems, are locations that are easily accessible to large numbers of people and that have limited security or protective measures in place making them vulnerable to attack. DHS has been working for many years to address ST-CP security and preparedness, with recent shifts in the threat landscape calling for renewed departmental focus on leveraging and maximizing its ST-CP security authorities, capabilities, and resources in an integrated and coordinated manner.

Cybersecurity and Infrastructure Security Agency Security of Soft Targets and Crowded Places—Resource Guide: Segments of our society are inherently open to the public, and by nature of their purpose do not incorporate strict security measures. Given the increased emphasis by terrorists and other extremist actors to leverage less sophisticated methods to inflict harm in public areas, it is vital that the public and private sectors collaborate to enhance security of locations such as transportation centers, parks, restaurants, shopping centers, special event venues, and similar facilities. The resource guide is a catalog of CISA soft target resources, many of which were created in collaboration with CISA's partners to ensure they are useful and reflective of the dynamic environment we live in. The resource guide is located here: www.dhs.gov/publication/securing-soft-targets-and-crowded-places-resources.

Soft Targets and Crowded Places Task Force (ST-CP TF): The ST-CP TF provides guidance to public and private sector partners to identify innovative means to increase security and mitigate risks the nation faces from terrorists or other violent extremist actors to soft targets and crowded places. The term ST-CP is typically defined as locations or environments that are easily accessible, attract large numbers of people on a predictable or semi-predictable basis, and may be vulnerable to attacks using simple tactics and readily available weapons. The Insider Threat Mitigation program is coordinated and consistent with standards set forth by the Department of Defense, Office of Director of National Intelligence - National Insider Threat Task Force (NITTF) and Carnegie Mellon University Software Engineering Institute.

Insider Threat (InT) Mitigation Web Site: The InT Mitigation web site provides a comprehensive step-by-step guide to developing an InT program, options for consideration for protecting assets, how to recognize and report an InT as well as assessing and responding to enhance security in workplace violence, cyber and physical threats. This resource is available at: www.dhs.gov/cisa/insider-threat-mitigation or intmitigation@hq.dhs.gov.

Understanding the Insider Threat video and trailer: The Insider Threat trailer (1 minute) and video (30 minutes) conveys the importance of a comprehensive InT program. The video uses security and behavior experts to discuss how insider threats manifest in a variety of ways including terrorism, workplace violence, and breaches of cybersecurity. Understanding how to recognize and respond to these various types of insider threats, whether non-violent or violent, increases an organization's ability to protect both its people and sensitive information. This resource is available at: www.dhs.gov/insider-threat-trailer-and-video#.

Pathway to Violence Video: The Pathway to Violence video provides information regarding the behavioral indicators that assailants often demonstrate before a violent act. Behavioral experts reference research conducted by Frederick Calhoun and Steve Weston on threat management and further describe the six progressive steps that may be observable by colleagues. The video also includes law enforcement expert interviews that discuss engagement strategies and recommended responses to someone potentially on a pathway to violence. This resource is available at: www.dhs.gov/pathway-violence-video.

Pathway to Violence Action Guide: The Guide explains warning signs that may lead to violence and what individuals can do to mitigate a potential incident. This resource is available at: www.dhs.gov/sites/default/files/publications/dhs-pathway-to-violence-09-15-16-508.pdf.

Insider Threat Fact Sheet: This fact sheet describes some of the Department of Homeland Security resources to help organizations design a comprehensive program that protects against workplace violence, and physical and cyber insider threats. This resource is available at: www.dhs.gov/publication/fact-sheet-insider-threat-mitigation-program.

Insider Threat Management Team Workshop (Pilot Phase): This workshop is currently being piloted with the regions and will be released in

the coming months. It is intended to serve as an in-person, field-delivered workshop focused on scenario-based training to assist organizations as they build multi-disciplinary teams to assess suspicious behavior and recommend appropriate actions to mitigate potential insider threats.

Options for Consideration Active Shooter Preparedness Video: The Options for Consideration video demonstrates possible actions that individuals can take if confronted with an active shooter scenario. This instructive video reviews the choices of running, hiding, or as an option of last resort, fighting the shooter. The video also shows how to assist authorities once law enforcement arrives. This resource is available at: www.dhs.gov/cisa/options-consideration-active-shooter-preparedness-video.

On-line Training: FEMA Emergency Management Institute Independent Study Courses: The below on-line training produced in coordination with CISA ST-CP TF, which includes Insider Threat security and awareness, are available at: www.dhs.gov/cisa/training-awareness.

- IS-906: Workplace Security Awareness
- IS-914: Surveillance Awareness: What You Can Do
- IS-915: Protecting Critical Infrastructure Against Insider Threats

Active Shooter Resources include 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. The desk reference guide, pocket card and poster are available on the following website, and is available in various different languages, to include Spanish at www.dhs.gov/cisa/human-resources-or-security-professional.

Interagency Security Committee : The ISC provides guidance to the federal facility security community on how to integrate Insider Threat activities within the organization and facility's overall security programs. This guidance is coordinated and consistent with the federal National Insider Threat Task Force.

Violence in the Federal Workplace: A Guide for Prevention and Response 2019: The importance of synchronizing a Workplace Violence program with an Insider Threat program is detailed in this guide which provides comprehensive information to assist in the creation of an effective workplace violence prevention and response program. This resource is available at: www.dhs.gov/publication/isc-violence-federal-workplace-guide.

Safeguarding and Securing Cyberspace

The Department has the lead for the federal government for securing civilian government computer systems, and works with industry and state, local, tribal and territorial governments to secure critical infrastructure and information systems. The Department works to: analyze and reduces cyber threats and vulnerabilities; distribute threat warnings; and coordinate the response to cyber incidents to ensure that our computers, networks, and cyber systems remain safe.

Cybersecurity Assessment Tools

The Cybersecurity and Infrastructure Security Agency (CISA) offers a dynamic suite of assessments through the Vulnerability Management and Coordination's (VMC) National Cybersecurity Assessments and Technical Services (NCATS) branch. Cyber Hygiene (CyHy) scans, Remote Penetration Testing (RPT), Risk and Vulnerability Assessments (RVA), Red Team Assessments (RTA), Validated Architecture Design Reviews (VADR), Critical Product Evaluations (CPE), and Security Architecture Review (SAR) assessments are all freely-available to federal, local, state, tribal, territorial, critical infrastructure and private sector agencies. These services will provide tactical mitigation of vulnerabilities while assisting stakeholders with maintaining a practical understanding of operational risks, challenges, and effective countermeasures which can assist with guiding data-driven strategies, policies, and initiatives. The CISA NCATS teams will work with stakeholders to implement technical and management/procedural capabilities, thereby reducing vulnerabilities in a measurable fashion to inform economic analysis efforts. For more information, please contact ncats_info@hq.dhs.gov.

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

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

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

Cyber Secure Dashboard (CSD) is organized according to the nationally accepted cybersecurity framework established by the

National Institute of Standards and Technology (NIST). Developed by the Critical Infrastructure Resilience Institute (CIRI), a DHS Center of Excellence led by the University of Illinois Urbana-Champaign, CSD cross references the DoD-mandated control requirements of the NIST SP 800-171 r1 with the cybersecurity control standard, the NIST SP 800-53r4. The goal of CSD is to provide concrete, best practices implementation guidance to simplify and expedite the process for every manufacturer, and to create a clear path to maintain future compliance. For more information, see www.ciri.illinois.edu or www.cybersecuredashboard.com/ or contact universityprograms@hq.dhs.gov.

Cyber Risk Scoring and Mitigation (CRISM) provides a mathematical approach to analyzing the cyber risks of a company's hardware and software systems. Developed by the CIRI, a DHS Center of Excellence led by the University of Illinois Urbana-Champaign, the tool scans network configurations and gives companies an overall picture of their network's vulnerabilities. CRISM analyzes and scores the exploitability of those vulnerabilities and provides a prioritized list of mitigation steps to be taken to reduce the risk and improve security. For more information, see www.ciri.illinois.edu or contact universityprograms@hq.dhs.gov.

Emergency Services Sector Cyber Risk Assessment (ESS-CRA) is the first ESS-wide cyber risk assessment completed under the NIPP framework, and it will inform collaborative and synchronized management of cyber risk across the sector. The ESS-CRA is intended to provide a risk profile that ESS partners can use to enhance the security and resilience of the ESS disciplines. By increasing the awareness of risks across the public and private sector domains, the ESS-CRA serves as a foundation for ongoing national-level collaboration to enhance the security and resilience of the ESS disciplines. The ESS-CRA is an initial effort to assess ESS cyber risks across the ESS disciplines and serves as a baseline of national-level risk. The assessment addresses those operational or strategic risks to the ESS infrastructure that are of national concern based upon the knowledge and subject matter expertise of those participating in the sector's risk assessment activities. The ESS-CRA describes an effort that required resources and coordination from across all disciplines of ESS to assess cyber risks to ESS critical infrastructure. This risk assessment provides the basis for an ESS cyber risk management plan or roadmap that will ensure that Federal resources are applied where they offer the most benefit for mitigating risk by lowering vulnerabilities, deterring threats, and minimizing the consequences of attacks and other incidents. The report also encourages a similar risk-based allocation of resources within State and local entities and the private sector. For more information, please contact essteam@hq.dhs.gov.

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

Cybersecurity Incident Resources, Detection, and Prevention Resources

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

Cyber Crimes Center (C3) ICE Homeland Security Investigations C3 supports the ICE HSI cyber mission through the programmatic oversight and coordination of investigations of cyber related criminal activity. ICE HSI C3 brings the full range of ICE HSI cyber investigations and computer forensic assets together in a single location to coordinate and support investigations into cyber related criminal activities; C3 is home to the Child Exploitation Investigations Unit, the Computer Forensics Unit, and the Cyber Crimes Unit. www.ice.gov/cyber-crimes.

Cyber Investigation Section (CIS) CIS is designed to target and proactively investigate major international criminals. This goal is accomplished through a combination of long-

term undercover operations, close partnerships with other U.S. government agencies, and consistently refined strategic targeting. In conjunction with this unique role, CIS has prototyped numerous advanced technical systems that allow for the integration and re-use of diverse forms of evidence from all U.S. jurisdictions and foreign partners. Also included under this unit are analysts and Criminal Research Specialists who focus on foreign language websites, money laundering activities, and digital/electronic currency. For more information, see www.secretservice.gov/ectf.shtml.

U.S. Secret Service Cyber Intelligence Section
CIS is a USSS Headquarters-based investigative unit focused on long term, strategic investigations and serving as a support network for field-based cyber investigations. The CIS investigative mission is to identify, locate, and apprehend high-value international cyber criminals involved in cyber intrusions, identity theft, credit card fraud, bank fraud, and other computer-related crimes. The information and coordination provided by CIS is a crucial element to successfully investigate, prosecute, and dismantle international criminal organizations.
CIS collects, analyzes, and disseminates data in support of Secret Service investigations worldwide and generates new investigative leads based upon this intelligence. CIS leverages technology and information obtained through private partnerships to monitor developing technologies and trends in cybercrime and their effects on the financial payments industry. The information acquired is used to enhance the Secret Service's capabilities to prevent and mitigate attacks against financial and critical infrastructures. CIS also leverages a team of full-time analysts who utilize foreign language capabilities (primarily Russian and related languages); in depth knowledge of online techniques and vernacular; and cutting-edge technological methods to expand the section's cyber investigative capabilities.
For more information, see www.secretservice.gov/ectf.shtml.

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

Enhanced Cybersecurity Services (ECS) The Cybersecurity and Infrastructure Security Agency's ECS program is a near real-time intrusion prevention and analysis capability that helps U.S.-based companies protect their computer systems against unauthorized access, exploitation, and data exfiltration. ECS works by sharing sensitive and classified cyber threat information with accredited Commercial Service Providers (CSPs). These CSPs in turn use that information to block certain types of malicious traffic from entering customer networks. The ECS program currently offers two innovative intrusion prevention services: Domain Name Service (DNS) Sink-holing and E-mail (SMTP) Filtering. For enrollment information, please contact the CSPs listed on the ECS webpage: www.dhs.gov/cisa/ecs.

Hunt and Incident Response Teams (HIRT)
The Cybersecurity and Infrastructure Security Agency provides free, onsite assistance to organizations needing immediate investigation and resolution of cyber-attacks. CISA members of HIRT can perform a preliminary diagnosis to determine the extent of compromise from a cyber-incident. At the customer's request, a team will visit the organization to review networks, identify infected systems, and collect data for follow-on analysis. HIRT provides mitigation strategies, helps restore service, and provides recommendations to improve overall network and control systems security. Learn more at www.dhs.gov/cisa/national-cybersecurity-communications-integration-center.

National Computer Forensics Institute (NCFI)
Is the result of a partnership between the Secret Service and the State of Alabama. The goal of this facility is to provide a national standard of training on a variety of electronic crimes investigations. This program will offer state and local law enforcement officers the training necessary to conduct computer forensics examinations, respond to network intrusion incidents, and conduct basic electronic crimes investigations. The NCFI will also train prosecutors, and judges on the importance of computer forensics to criminal investigations. This training acts as a force

multiplier for the Secret Service and other federal law enforcement agencies, thus reducing the volume of cybercrime cases impacting the federal judicial process. For more information, see www.ncfi.usss.gov.

National Cyber Awareness System the US-CERT National Cyber Awareness System offers a variety of up-to-date information on general cybersecurity topics, threats and vulnerabilities via subscription lists and feeds for alerts, bulletins, and tips. For more information, visit www.us-cert.gov/cas/ or contact info@us-cert.gov 888-282-0870.

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

Industrial Control Systems (ICS) Support The Cybersecurity and Infrastructure Security Agency partners with and serves the industrial control systems community to reduce risk to these unique, potentially high-risk systems. Industrial control systems are defined as the devices, systems, networks, and controls used to operate and/or automate industrial processes. CISA plays a critical role by coordinating efforts among government and control system owners, operators, and vendors on vulnerabilities, threats, and risks. CISA leads the ICS Joint Working Group (ICSJWG) to facilitate information sharing and reduce the risk to the nation's industrial control systems. For more information, visit www.us-cert.gov/ics/Industrial-Control-Systems-Joint-Working-Group-ICSJWGw.

Malware Analysis and Response CISA collects, analyzes, and exchanges malware information 24 hours a day. Participants can submit malware artifacts (tools, malicious code, other attack technology, or indications like access statistics indicating a possible DNS attack) electronically to CISA. Learn more at www.dhs.gov/how-do-i/report-cyber-incidents.

Cybersecurity and Infrastructure Security Agency's Enhanced Cybersecurity Services (ECS) Program provides near real-time intrusion prevention and analysis to help U.S.-based companies and state and local governments protect systems against unauthorized access, exploitation, and data theft. ECS shares sensitive and classified cyber threat information with accredited Commercial Internet Service Providers who then block malicious traffic from customer networks. ECS does not replace but augments an organization's existing cybersecurity resources by providing an additional layer of defense against known or suspected cyber threats, while also providing early detection of potential compromise. Learn more at www.dhs.gov/cisa/enhanced-cybersecurity-services-ecs.

Cybersecurity Technical Resources

Cyber Essentials The Cybersecurity and Infrastructure Security Agency's Cyber Essentials is a guide for leaders of small businesses as well as leaders of small and local government agencies to develop an actionable understanding of where to start implementing organizational cybersecurity practices. Consistent with the National Institute of Standards and Technology's Cybersecurity Framework and other standards, the Cyber Essentials are the starting point to cyber readiness. Reducing an organization's cyber risk requires a holistic approach, similar to that taken to address other operational risks. For more information visit www.cisa.gov/cyber-essentials

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

Cyber Exercise Program (CEP) was established in 2004 to strengthen the reliability and resiliency of the Nation's critical cyber infrastructure through the development, design, and conduct of scenario-based cyber exercises. The CEP can build a

Cyber Tabletop Exercise Package (CTEP) for most any critical infrastructure/key resource sector and has already co-produced CTEPs for the Chemical, Critical Manufacturing, and the Healthcare and Public Health Sectors. The CTEP provides organizations all the materials needed to plan and conduct a discussion-based cyber exercise. The CTEP includes two scenarios designed to help assess security policies and procedures for both the "business" and "operational" aspects of an organization. Highly customizable, it gives the planner the flexibility to use organizational goals and objectives, or choose goals and objectives included in the package. Also included in the package are planning guides, templates, checklists to guide and track the planning process, Situation Manuals, and post-exercise instructions. For more information, please contact cep@dhs.gov.

Cybersecurity Strategy Development The Cybersecurity and Infrastructure Security Agency's National Cyber Exercise and Planning Program (NCEPP) was established in 2004 to increase cyber preparedness and resilience across the entire spectrum of DHS stakeholders. They develop and support integrated cyber-focused exercises and guidance for Federal departments and agencies, state, local, tribal, and territorial governments, critical infrastructure sectors, international partners, and special events. Following DHS's Homeland Security Exercise and Evaluation Program (HSEEP) model, NCEPP plans cyber exercises tailored to its public and private sector partners on an as-needed and as-available basis. Exercises range from small-scale, limited-scope, discussion-based exercises (e.g., two-hour seminars) to large-scale, internationally-scoped, operations-based exercises (e.g., multi-day, full-scale exercises). NCEPP offers the following services at no cost: National Level Exercises, including Cyber Storm and Tabletop the Vote, end-to-end cyber exercise planning and conduct, cyber exercise consulting and subject matter expert support, cyber planning support, and off-the-shelf resources. For entities that prefer to develop their own exercises, NCEPP provides subject matter experts to consult on exercise design and development. These subject matter experts can review scenarios, participate in planning calls, and provide exercise controller and/or observer support. For more information, please contact cep@dhs.gov.

Department of Homeland Security Science and Technology Directorate Physical and Cyber Security (DHS S&T PCS) develops and transitions new technologies, tools, and techniques to protect and secure systems, networks, infrastructure, and users, improving the foundational elements of our nation's critical infrastructure and the world's information infrastructure; and, to provide coordination and leadership for research and development across federal, state, and municipal governments, international partners, the private sector, and academia to improve cybersecurity research infrastructure. DHS S&T PCS frequently works with the private sector to develop requirements and engage transition partners for the tools, technologies and techniques that result from PCS's work. For more information about PCS and its specific projects, workshop information and presentations, cybersecurity news, events and outreach information, see www.cyber.st.dhs.gov/ or contact sandt-cyber-liaison@hq.dhs.gov.

Cybersecurity in the Gaming Subsector Webinar focused on cybersecurity threats, vulnerabilities, and best practices specific to the gaming and casino industry. More than 100 gaming industry representatives participated in the Webinar, which was designed to raise awareness of cybersecurity within the Gaming Subsector. The Critical Infrastructure Protection Cybersecurity (CIP CS) program and I&A discussed some of the latest cyber threats specific to the Gaming Subsector and steps industry can take to improve their cyber resilience. These steps include managing employees to mitigate insider threats, communicating with gaming machine vendors about vulnerabilities, securing newly digital IP surveillance systems, and conducting cybersecurity assessments. For more information, email ncsd_cipcs@hq.dhs.gov.

Cybersecurity in the Retail Subsector Webinar provides retail employees and managers with an overview of the cyber threats and vulnerabilities facing the industry. The webinar also reviews the types of cyber systems and infrastructure used by the retail industry and steps that retail personnel can take to address the unique vulnerabilities to those cyber resources. For more information contact cfsteam@hq.dhs.gov.

Industrial Control Systems Cybersecurity Training is provided through either 8-hour

lessons through a virtual learning portal or 5-day instructor led training for control system and IT professionals. Course goals include risk reduction for control systems in critical infrastructure, identification of DHS tools and resources, and coordination of event management with DHS. For more information, visit www.us-cert.gov/ics/training-available-through-ics-cert#need.

The Cybersecurity Assessment and Risk Management Approach (CARMA), created by the National Cyber Security Division's (NCSD) Critical Infrastructure Protection Cyber Security (CIP CS) program, developed a flexible, repeatable, and reusable cyber risk management approach to help CIKR sectors, state and local governments, and other public and private sector organizations manage cyber critical infrastructure risk. CARMA incorporates lessons from a wide variety of cyber risk management activities. CARMA accounts for the virtual and distributed nature of cyber critical infrastructure and the complexity of the missions and services it supports; considers strategic security goals and can guide all levels of cyber risk efforts; and allows infrastructure owners and operators to integrate their established cyber risk frameworks into the approach or use the approach as a foundation for broader enterprise risk management efforts. CARMA is a comprehensive, functions-based risk management strategy that focuses on cyber critical infrastructure and effectively identifies, assesses, and manages shared risks. For more information, email ncsd_cipcs@hq.dhs.gov.

Cybersecurity Education and Workforce Development Program (CEWD) fosters effective cybersecurity education and workforce development programs by facilitating the availability of professionals qualified to support the nation's cybersecurity needs. To support national cybersecurity workforce development, CEWD developed the IT Security Essential Body of Knowledge (EBK), an umbrella framework that links competencies and functional perspectives to IT security roles to accurately reflect a national perspective. For more information, see www.us-cert.gov/itsecurityebk/.

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

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

Cybersecurity Information Products and Recommended Practices provide current cybersecurity information resources and recommend security practices to help industry understand emerging control systems cyber security issues and mitigate vulnerabilities. This information will help users reduce their exposure and susceptibility to cyber-attacks and exploits. For a complete list and access to cybersecurity information products, visit www.us-cert.gov/control_systems/csdocuments.html.

Cybersecurity Webinars, as an information sharing mechanism, can increase the level of participation and activity among public and private sector stakeholders by engaging them in a cybersecurity discussion. The National Cyber Security Division's Critical Infrastructure Protection Cyber Security (CIP-CS) Program can help plan, coordinate, and execute a cybersecurity webinar in partnership with sector stakeholders by identifying webinar topics to address goals and objectives; assisting the host organization with determining participants, timeframe, and speakers; developing a webinar outline; inviting other Department of Homeland Security (DHS) components to participate and coordinate on topics of interest; and working with the sponsoring sector or organization to provide follow-up materials. CIP-CS has partnered with the Commercial Facilities and

Emergency Services Sectors to produce webinars. For more information, email ncsd_cipcs@hq.dhs.gov.

Domain Name System Security Extensions (DNSSEC) Deployment Coordinating Initiative provides cryptographic support for domain name system (DNS) data integrity and authenticity. DHS sponsors a community-based, international effort to transition the current state of DNSSEC to large-scale global deployment, including sponsorship of the DNSSEC Deployment Working Group, a group of experts active in the development or deployment of DNSSEC. It is open for anyone interested in participation. The DNSSEC website contains articles, published research papers, DNSSEC tools, case studies, workshop information, and presentation materials. For more information, see www.dnssec-deployment.org/.

Industrial Control System Cybersecurity Standards and References provide an extensive collection of cybersecurity standards and reference materials as a ready resource for the industrial control system stakeholder community. To view the collection, visit www.us-cert.gov/ics/Standards-and-References.

Information Technology Sector Specific Plan (IT SSP) outlines the IT Sector security partners' joint implementation of the NIPP risk management framework. It describes an approach for identifying, assessing, prioritizing, and protecting critical IT Sector functions, establishing shared IT Sector goals and objectives, and aligning initiatives to meet them. To view the IT SSP, visit www.dhs.gov/sector-specific-plans. For more information, contact ncsd_cipcs@hq.dhs.gov.

The National Cyber Security Division's (NCSD) Critical Infrastructure Protection Cyber Security (CIP-CS) program developed a flexible, repeatable, and reusable cyber risk management approach to help CIKR sectors, state and local governments, and other public and private sector organizations manage cyber critical infrastructure risk. This approach—the Cybersecurity Assessment and Risk Management Approach—incorporates lessons from a wide variety of cyber risk management activities. CARMA is a comprehensive, functions-based risk management strategy that focuses on cyber critical infrastructure and effectively identifies, assesses, and manages shared risks. For more information, email ncsd_cipcs@hq.dhs.gov.

Network Security Information Exchange (NSIE) The NSTAC recommended the establishment of an Industry-government partnership to reduce the vulnerability of the Nations' telecommunications systems to electronic intrusion. The NSTAC formed separate government and industry NSIEs to share ideas on technologies and techniques for addressing and mitigating the risks to the public network and its supporting infrastructures. For more information, visit www.dhs.gov/publication/nsie-fact-sheet.

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

Open Source Infrastructure Cyber Read File compiles important cybersecurity and cyber infrastructure news articles across CIKR sectors and provides a repository of cybersecurity open source information. The Read Files are intended to increase awareness of cybersecurity issues—thus aiding sectors during strategic cybersecurity risk management planning. Modeled on the Department of Homeland Security's Daily Open Source Infrastructure Report, the monthly Open Source Infrastructure Cyber Read File focuses on cybersecurity and cyber infrastructure. Articles are drawn from open source news resources and are organized by date and the sector(s) they affect. In the Open Source Infrastructure Cyber Read File, CIP CS applies knowledge of how issues could inform sectors' strategic planning efforts by including contextual information in addition to the news article. The additional context helps increase understanding of how cybersecurity impacts critical infrastructure protection efforts. Sector-Specific Agencies and other organizations, including State and Federal government agencies, may share the Read File with their stakeholders, many of whom may not be aware of cybersecurity issues relevant to their activities. For more

information, email ncsd_cipcs@hq.dhs.gov.

The Information Marketplace for Policy and Analysis of Cyber-Risk & Trust (IMPACT) is the only freely-available legally collected and distributed repository of large-scale cybersecurity data and analytics tools, allowing researchers to advance the state-of-the-art in cyber-risk R&D and decision support. The intent is to accelerate design, production, and evaluation of next-generation cyber security solutions, including commercial products. Data providers legally provide the data to be shared through the repository, data hosts provide the infrastructure to store the repository data and transfer it to authorized recipients, and the coordinating center provides a centralized mechanism for cataloging available data and manages the submission and review of data requests. The goal of the distributed structure is to provide secure, centralized access to multiple sources of data and promote data sharing while protecting the privacy of the data producers and the security of their networks and data. IMPACT continually adds new data containing the latest cybersecurity attacks so that the research community will have the most recent information to help improve the quality of research results. For more information, visit www.impactcybertrust.org/.

Nuclear Sector Cybersecurity Framework Implementation Guidance The Nuclear Sector Cybersecurity Framework Implementation Guidance serves as a resource for the Nuclear Sector to effectively prioritize and apply cybersecurity principles laid out in the National Institute of Standards and Technology's 2014 Framework for Improving Critical Infrastructure Cybersecurity. It provides tools and resources tailored to the nuclear industry to allow users to identify, assess, and manage sector-specific cybersecurity risks, threats, and vulnerabilities. For more information, please contact the Nuclear Security Specific Agency at nuclearssa@hq.dhs.gov.

Roadmap to Enhance Cyber Systems Security in the Nuclear Sector The Roadmap to Enhance Cyber Systems Security in the Nuclear Sector describes coordinated activities to improve cyber systems security in the Nuclear Sector. It provides nuclear control and cyber systems vendors, asset owners and operators, and relevant government agencies, with a common vision, goals, and objectives for cyber systems security in the sector. It also provides milestones to focus specific efforts and activities for achieving the vision, goals, and objectives over the next 10 to 15 years, addressing the Nuclear Sector's most urgent challenges, as well as its longer-term needs to reduce the cyber security risk to nuclear industrial cyber systems. For more information, please contact the Nuclear Sector Specific Agency at nuclearssa@hq.dhs.gov.

Roadmap to Secure Control Systems in the Chemical Sector 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. For more information, please contact the Chemical Sector Specific Agency at chemicalsector@hq.dhs.gov.

Information Sharing

Automated Indicator Sharing (AIS) enables real-time, bi-directional exchange of cyber threat indicators with the goal of reducing the number of cyber-attacks. For more information, visit www.dhs.gov/cisa/automated-indicator-sharing-ais.

Cyber Information Sharing and Collaboration Program (CISCP) is a voluntary information-sharing program among critical infrastructure and the Federal Government. The program builds a community of trust and enhances collaboration between participants. For more information, visit www.dhs.gov/cisa/cyber-information-sharing-and-collaboration-program-ciscp.

Software Assurance (SwA)

Software Assurance Program (SwA) Software Assurance is the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted and that software applications function in the intended manner. Grounded in the National Strategy to Secure Cyberspace, the SwA Program develops practical guidance and tools, and promotes research and development of secure software engineering. Resources including articles, webinars, podcasts, and tools for software

security automation and process improvement are constantly updated at the SwA Community Resources and Information Clearinghouse located at https://buildsecurityin.us-cert.gov/swa/. For more information, contact software.assurance@dhs.gov.

Automating Software Assurance Under SwA sponsorship, MITRE, in collaboration with government, industry, and academic stakeholders, is improving the measurability of security through enumerating baseline security data, providing standardized languages as means for accurately communicating the information, and encouraging sharing of this information with users by developing repositories (see Security Automation & Measurement: http://buildsecurityin.us-cert.gov/swa/measurable.html). Sponsored by the Software Assurance Program, MITRE issues electronic newsletters and information on the following technologies employed in automating SwA: Common Vulnerabilities and Exposures (CVE); Common Weakness Enumeration (CWE); Common Attack Pattern Enumeration and Classification (CAPEC); Open Vulnerability and Assessment Language (OVAL); and Malware Attribute Enumeration and Characterization (MAEC). Structured Threat Information eXpression (STIX) is a quickly evolving, collaborative community-driven effort to define and develop a language to represent structured threat information. The STIX language is meant to convey the full range of cyber threat information and strives to be fully expressive, flexible, extensible, automatable, and as human-readable as possible. It is actively being adopted or considered for adoption by a wide range of cyber threat-related organizations and communities around the world. All interested parties are welcome to participate in evolving STIX as part of its open, collaborative community and leverage the upcoming STIX web site and collaborative forums. For more information, see www.mitre.org/work/tech_papers/2010/10_1420/10_1420.pdf.

Resilient Software Assurance promotes the security and resilience of software across the development, acquisition, and operational lifecycle; as such, SwA is scoped to address Trustworthiness, Dependability (correct and predictable execution), Conformance, and Survivability. The focus on Resilience and Survivability enables stakeholders to understand and proactively act to design, build, acquire, and operate software and software-enabled services with knowledge that software must be able to operate in non-benign environments. Moreover, if compromised, damage to the software will be minimized and it will recover quickly to an acceptable level of operating capacity; it's "rugged." Several initiatives have focused on developing rugged software that is attack-aware and self-defending. See https://buildsecurityin.us-cert.gov/swa/resilient.html for details.

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

Software Assurance (SwA) Resources To support SwA in higher education, SwA and the Software Engineering Institute (SEI) have developed Software Assurance Curriculum Materials (https://buildsecurityin.us-cert.gov/swa/mswa.html) which are freely available for download. This curriculum is formally recognized by the Institute of Electrical and Electronics Engineers (IEEE) and the Association for Computing Machinery (ACM). At the Forum and Working Group Sessions, SwA distributes CDs of SwA resources. Included on the CDs are guides, reports, and brochures on numerous topics such as:

- SwA Capability Benchmarking Documents (https://buildsecurityin.us-cert.gov/swa/proself_assm.html)
- SwA Ecosystem Page (https://buildsecurityin.us-cert.gov/swa/ecosystem.html)

- FAQs and Fact Sheets on SwA Forums and Working Groups (https://buildsecurityin.us-cert.gov/swa/faq.html)
- Whitepapers from the Software Assurance Community (https://buildsecurityin.us-cert.gov/swa/ttpe_research.html)
- Evaluating and Mitigating Software Supply Chain Security Risk, May 2010 (https://buildsecurityin.us-cert.gov/swa/downloads/MitigatingSWsupplyChainRisks10tn016.pdf)
- SwA Pocket Guide Series - free, downloadable documents on critical software assurance topics (https://buildsecurityin.us-cert.gov/swa/pocket_guide_series.html).

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

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

Software Assurance (SwA) Outreach As part of an extensive outreach effort, the SwA participates in conferences and webinars with the International Information Systems Security Certification Consortium (ISC)², the Information Systems Security Association, Open Web Application Security Project (OWASP), and other organizations interested in application security. More about SwA relevant webinars is available on the BSI and CRIC websites. For more information, visit https://buildsecurityin.us-cert.gov/swa/webinars.html. Moreover, SwA supports online communities of interest, such as the Software Assurance Education Discussion Group on LinkedIn at www.linkedin.com/groups?mostpopular=&gid=3430456 and the Software Assurance Mega-Community at www.linkedin.com/groups?home=&gid=1776555&trk=anet_ug_hm.

The Top 25 Common Weakness Enumerations (CWE) In cooperation with the System Administration, Audit, Network Security (SANS) Institute, SwA and MITRE issued the report, "Improve Security and Software Assurance: Tackle the CWE Top 25 – The Most Dangerous Programming Errors." The Top 25 CWEs represent the most significant exploitable software constructs that have made software so vulnerable. Communicating and addressing these problematic issues will serve to improve software security, both during development and while in operation. Read more and see the list of "Top 25 CWE Programming Errors" at https://buildsecurityin.us-cert.gov/swa/cwe/.

Securing and Managing Our Borders

The Department of Homeland Security secures the nation's air, land, and sea borders to prevent illegal activity while facilitating lawful travel and trade. The Department's border security and management efforts focus on three interrelated goals: effectively secure U.S. air, land, and sea points of entry; safeguard and streamline lawful trade and travel; and disrupt and dismantle transnational criminal and terrorist organizations.

Border and Economic Security

1-800 BE ALERT The public can report suspicious activity to the U.S. Customs and Border Protection via a toll free telephone reporting system. To report suspicious activity: Call 800-BE ALERT or 800-232-5378. For more information on U.S. Border Patrol Checkpoints call 877-227-5511. International Callers dial +1 703-526-4200.

CBP deploys the government's largest law enforcement workforce to protect at and between ports of entry, supported by air and marine assets. For more information on CBP, visit www.cbp.gov.

CBP Laboratories and Scientific Services coordinates technical and scientific support to all CBP trade and border protection activities. For more information, visit www.cbp.gov/about/labs-scientific-svcs.

CBP Newsroom, News Magazine and Alerts compiles the latest information on noteworthy occurrences documenting apprehensions of criminals, seizures of illegal drugs, rescues missions, and many other agency success stories from around the country. These highlights can be found at www.cbp.gov/newsroom.

DHS Center of Excellence: The Borders, Trade, and Immigration (BTI) Institute, led by the University of Houston, conducts and transitions research, develops innovative solutions, and provides education that enhances the Nation's ability to secure the borders, facilitate legitimate trade and travel, and ensure the integrity of the immigration system. The BTI Institute delivers transformational technology-driven solutions, data-informed policies, workforce development opportunities for today's Homeland Security Enterprise. For more information, see www.uh.edu/bti/ or contact universityprograms@hq.dhs.gov.

DHS Center of Excellence: Criminal Investigations and Network Analysis (CINA) Center, led by George Mason University, develops strategies and solutions to enhance criminal network analysis, forensics, and investigative processes for on-the-ground use by agents and officers to counteract transnational crime. For more information, see https://cina.gmu.edu or contact universityprograms@hq.dhs.gov.

DHS Center of Excellence: Cross Border Threat Screening and Supply Chain Defense (CBTS) Center, led by Texas A&M University, assists DHS operations that protect the global supply chain and reduce the risk of exposing people and infrastructures to new and evolving biological threats to the nation's people, agriculture, and economy. For more information, contact universityprograms@hq.dhs.gov.

eAllegations provides concerned members of the public a means to confidentially report suspected trade violations to CBP. For more information, or to initiate an investigation, visit https://eallegations.cbp.gov or contact the Trade Remedy Law Enforcement Office of International Trade at: 800-BE-ALERT (800-232-5378).

Highway and Motor Carrier First Observer ™ Call-Center "First Observer" trained specialists serve as the first line of communication for all matters related to this anti-terrorism and security awareness program. Well trained responders provide nationwide first responder and law enforcement contact numbers and electronic linkage to registered participants. Reported caller information is entered into a secure reporting system that allows for an electronic transfer to the Information Sharing and Analysis Center (ISAC) for further investigation by industry analysts. The call center may also be utilized during an incident of national significance. Call the center 24 x 7 888-217-5902. For more information, see www.firstobserver.com.

Homeland Security Investigations (HSI) Tip-line is a 24x7 centralized intake center established to receive tips from the public and law enforcement. The Tip-line receives, analyzes, documents, and disseminates tip information regarding more than 400 laws enforced by the Department of Homeland Security. Highly trained intelligence research specialists have the knowledge and experience to quickly disseminate actionable leads to the responsible DHS field office, both in the United States and to HSI attaché offices around the world. With broad access to law enforcement and commercial computer databases, Tip-line specialists can enhance tip information prior to forwarding to the responsible field office. With real-time access to interpreter services, information can be collected using more than 300 languages. The Tip-line can also quickly connect federal, state, local, and tribal law enforcement officers with their local HSI duty agent. To contact the HSI Tip-line, call toll free 866- 347-2423 or use the internet-based HSI

Tip Form at www.ice.gov/tips. Also available is a "widget" that can be placed on the websites of partner organizations and companies to allow for one-click access to the HSI Tip Form.

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

Operation Stonegarden Grant Program (OPSG) OPSG funds are intended to enhance cooperation and coordination among local, tribal, territorial, state, and federal law enforcement agencies in a joint mission to secure the United States' borders along routes of ingress from international borders to include travel corridors in states bordering Mexico and Canada, as well as states and territories with international water borders. For more information, see www.fema.gov/homeland-security-grant-program.

Project Shield America is the first line of defense against those who compromise U.S. national security by violating export laws, sanctions and embargoes. Specifically, the ICE Counter-Proliferation Investigations Unit reaches out to applicable high-tech industries to monitor weapons of mass destruction and their components that are potential targets for illegal trafficking. Through Project Shield America, ICE works in partnership with U.S. Customs and Border Protection and U.S. companies that manufacture, sell or export strategic technology and munitions. For more information, see www.ice.gov/project-shield-america or contact ICE headquarters, Project Shield America program manager at (703) 287-6900.

Trade Facilitation

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

Automated Commercial Environment (ACE) is the commercial trade processing system that connects CBP, the international trade community and PGAs. It is the U.S. Single Window, the primary processing system through which trade-related data required by all government agencies is submitted and processed. ACE facilitates legitimate trade while strengthening border security by providing government officials with better automated tools and information. All import manifest, cargo release, post release, export and PGA integration functionality scheduled for delivery in ACE is now available. For more information about ACE, visit www.cbp.gov/trade/automated.

Automated Commercial Environment (ACE) Account Service Desk provides customer technical support services 24 hours a day, 7 days a week, including information about ACE Secure Data Portal account access, account management, and running ACE Reports. The ACE Help Desk is the first point of contact for all ACE users experiencing system difficulties. To reach the ACE Help Desk, call 866-530-4172 or email ACE.Support@cbp.dhs.gov

Automated Commercial System (ACS) is CBP's legacy automated import processing system that has been primarily retired as import processing capabilities have been transitioned to the Automated Commercial Environment (ACE). Currently, electronic entry payment/collection processes and a limited set of data queries are still conducted in ACS, however CBP is in the process of migrating this functionality to ACE. For more information, see www.cbp.gov/trade/acs/catair or contact 571-468-5000.

Cargo Systems Messaging Service (CSMS) is a messaging platform for distributing timely service messages to automated cargo systems users as well as courtesy messages on related trade processing information. To receive CSMS messages, subscribe at: https://csms.cbp.gov/csms.asp?display_page=1.

CBP Client Representatives are the first points of contact for importers, exporters, transportation providers, and brokers wishing to automate any of their Customs processes. Client Representatives are the contact point for all system-related problems and questions from trade partners. For more information, see www.cbp.gov/trade/automated/getting-started/transmitting-data-cbp-electronic-data-

interchange-edi.

CBP INFO Center Self Service Q&A Database is a searchable database with over 600 answers to questions about CBP programs, requirements, and procedures. If visitors to the site are unable to find an answer to their question, they may also submit an inquiry or complaint for personal assistance. To use the searchable database, visit https://help.cbp.gov/app/home or call the CBP INFO Center at 877-CBP-5511 or 703-526-4200.

CBP Trade Outreach The Office of Trade Relations (OTR) serves as the CBP point of contact for the international trade community by supporting communications between CBP and the private sector. Situated within the Office of the Commissioner, OTR is responsible for industry engagement, dissemination of information, and solicitation of input from the private sector and PGAs to include new importers, exporters and small businesses. For more information, visit www.cbp.gov/trade/stakeholder-engagement/trade-relations.

CBP Small Business Regulatory Fairness Representative The Executive Director Trade Relations for U.S. Customs and Border Protection was selected by the Commissioner to serve as the Regulatory Fairness Representative for the agency and is responsible for performing as the link between the international trading community and senior CBP managers. In addition, the Executive Director of Trade Relations is responsible for policy review, planning and counsel to the Commissioner, Department of Homeland Security, and Congress on the quality of service provided to the trade community. As the official representative, the Executive Director of Trade Relations will promote compliance with Small Business Regulatory Enforcement Fairness Act (SBREFA) and, to the extent possible, the recommendations of the National Ombudsman and the Regional Regulatory Fairness Boards. Should you have any concerns which you feel have not been resolved in an appropriate manner, contact the Executive Director of Trade Relations at: www.cbp.gov/trade/stakeholder-engagement/user-fee-advisory-committee.

CBP/USCG Joint Protocols for the Expeditious Recovery of Trade The *CBP/USCG Joint Protocols for the Expeditious Recovery of Trade* inform national level decision-making to facilitate the stabilization and recovery of basic functions of the marine transportation system (MTS) after a Transportation Disruption as defined by the *SAFE Port Act of 2006*. The protocols are activated when needed as an engagement forum among national level maritime industry associations, CBP, the U.S. Coast Guard, and other federal agencies with maritime trade responsibilities to inform federal decision-making. The protocols 1. support Presidential Directives that pertain to maritime security and the protection of the national economy and national defense,2. establish a national level communications process to be employed by the U.S. Coast Guard, CBP, and other federal agencies, as well as the maritime industry, following or prior to an event that causes a major disruption to the MTS, 3. consider the collateral impacts of a major disruption of the MTS on international commerce, 4. support federal decision-making and the protection of federal interests, and 5. establish how the U.S. Coast Guard and CBP will interact with other government agencies to jointly facilitate the expeditious recovery of the national MTS and the resumption of commerce in support of the DHS *Global Supply Chain Security Strategy*. At the port level, maritime industry engagement in trade recovery is accomplished through incident management structures that are mobilized on a case by case basis and are dependent upon the severity of an incident impacting the local components of the MTS within a U.S. Coast Guard Captain of the Port (COTP) Zone. For more information, call 202-372-1092 or visit the U.S. Coast Guard's Office of Port and Facility Compliance (CG-FAC) webpage, www.dco.uscg.mil/our-organization/assistant-commandant-for-prevention-policy-cg-5p/inspections-compliance-cg-5pc/cgfac/.

Customs Rulings Online Search System (CROSS) is a searchable database of CBP rulings that can be retrieved based on simple or complex search characteristics using keywords and Boolean operators. CROSS has the added functionality of CROSS referencing rulings from the initial search result set with their modified, revoked or referenced counterparts. Rulings collections are separated into Headquarters and New York and span the years 1989 to present. Collections can be searched individually or collectively. For more information, see https://rulings.cbp.gov/home.

Customs-Trade Partnership Against Terrorism (CTPAT) is a voluntary government-business initiative developed in order to strengthen and improve the international supply chain to increase U.S. border security against the threat

of terrorism. Through CTPAT, businesses in the program ensure the integrity of their security practices, communicate, and verify the security criteria of their business partners within the supply chain. For more information, or to apply online, visit www.cbp.gov/ctpat. You may also email the program at OFO-INDUSTRYPARTNERSHIP@cbp.dhs.gov

Importer Self-Assessment Program (ISA) has now transitioned into the **CTPAT Trade Compliance program (TC)** as of October 2019. The TC program provides the opportunity for importers to assume responsibility for monitoring their own compliance. Public information regarding this program, including frequently asked questions, policy information, best practices, and requirements can be found at www.cbp.gov/trade/trade-community/outreach-programs/trade-program-contacts/CTPAT-poc

Informed Compliance Publications are available on a specific trade issues, and summarize practical information for the trade community to better understand their obligations under customs and related laws. For more information, see website link www.cbp.gov/trade/rulings/informed-compliance-publications.

Red Lists of Cultural Objects at Risk
Red Lists present the categories of cultural objects that can be subjected to theft and traffic. They help individuals, organizations and authorities, such as police or customs officials, identify objects at risk and prevent them from being illegally sold or exported. For more information, visit https://icom.museum/en/activities/heritage-protection/red-lists/.

Secure Freight Initiative (SFI) and Importer Security Filing and additional carrier requirements (10+2) The Secure Freight Initiative, through partnerships with foreign governments, terminal operators, and carriers, enhances the DHS capability to assess the security of U.S.-bound maritime containers by scanning them for nuclear and other radioactive materials before they are laden on vessels bound for the U.S. For more information, please visit www.cbp.gov/border-security/ports-entry/cargo-security/importer-security-filing-102 or contact securefreightinitiative@dhs.gov.

Travel Facilitation

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

Entry Process into United States CBP welcomes more than 1.1 million international travelers into the United States at land, air, and sea ports on an average day. U.S. citizens and international visitors may consult publications and factsheets for information to simplify their entry into the U.S. For information about international travel, Contact the CBP Information Center at 877-227-5511.

Global Entry, one of the CBP trusted traveler programs, allows pre-approved, low-risk travelers expedited clearance upon arrival into the U.S. Although this program is intended for "frequent travelers" who make several international trips per year, there is no minimum number of trips an applicant must make to qualify. For more information, visit www.globalentry.gov, or contact cbp.goes.support@dhs.gov 866-530-4172.

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

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

TSA Pre✓® Application Program The TSA Pre✓® Application Program, one of the DHS Trusted Traveler programs, allow pre-approved, low-risk travelers to use expedited screening lanes at U.S. airports for domestic travel and departures from a U.S. airport to a foreign country. For more information about the TSA Pre✓® Application Program, visit

https://www.tsa.gov/precheck. To enroll, visit https://universalenroll.dhs.gov/workflows?servicecode=11115V&service=pre-enroll.

Western Hemisphere Travel Initiative (WHTI) requires citizens of the U.S., Canada, and Bermuda to present a passport or other acceptable document that denotes identity and citizenship when entering the U.S. For more information about WHTI, visit https://www.cbp.gov/travel/us-citizens/western-hemisphere-travel-initiative/faqs or contact CBP INFO Center at 877-227-5511 or 703-526-4200, TDD: 866-880-6582.

INDEX

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

Y