

# Private Sector Resources Catalog

*May 2012*



Homeland  
Security

Intentionally blank page. Please continue to the next page.

# Contents

<b>Letter from Assistant Secretary Douglas A. Smith.....</b>	<b>5</b>
<b>Department-wide Resources .....</b>	<b>6</b>
Civil Rights, Civil Liberties, and Privacy .....	6
Economic Analysis.....	8
Outreach and Engagement .....	8
Policy Guidance.....	11
Research and Product Development .....	12
Protecting Against Fraud & Counterfeiting.....	15
Social Media Engagement.....	17
<b>Preventing Terrorism and Enhancing Security .....</b>	<b>18</b>
Aviation Security .....	18
Bombing Prevention .....	19
Chemical Security.....	21
Critical Infrastructure – Multiple Sectors.....	23
Critical Manufacturing .....	24
Commercial Facilities .....	25
Dams Security .....	26
Food Safety and Influenza.....	28
Hazardous Materials Transportation Security .....	28
Land Transportation and Pipeline.....	29
Maritime Security .....	31
Mass Transit and Rail Security .....	32
Nuclear Security.....	34
Physical Security Assessment Tools .....	35
Protecting, Analyzing, & Sharing Information.....	36
<b>Securing and Managing Our Borders.....</b>	<b>40</b>
Border Security .....	40
Trade Facilitation .....	41
Travel Facilitation.....	42
<b>Enforcing and Administering Our Immigration Laws.....</b>	<b>43</b>
Immigration Questions and Concerns.....	43
Immigration .....	43
Employment Eligibility Verification .....	44
Immigration Enforcement.....	45
<b>Safeguarding and Securing Cyberspace .....</b>	<b>46</b>
Cybersecurity Assessment Tools .....	46
Cybersecurity Incident Resources .....	46
Cybersecurity Technical Resources.....	47
Software Assurance (SwA) .....	49
<b>Ensuring Resilience to Threats and Hazards.....</b>	<b>51</b>
Business Preparedness.....	51

Emergency Communications .....	52
Emergency Responder Community.....	54
Personal and Community Preparedness .....	56
<b>Appendix A – Key Contacts .....</b>	<b>59</b>
<b>Appendix B – Index .....</b>	<b>63</b>

# Letter from Assistant Secretary Douglas A. Smith



**Homeland  
Security**

May 22, 2012

Dear Private Sector Partner,

Two years after its original debut, I am pleased to release the newly updated Private Sector Resources Catalog. The breadth and depth of resources created by DHS to support our private sector partners is truly amazing, and we have created this catalog to make your access to those resources easier. This update features many completely new resources, along with a more comprehensive index that not only organizes resources by critical infrastructure sector but that also reflects some of the new preparedness terminology under Presidential Policy Directive 8: National Preparedness. As we continue to make this document as useful as possible, we welcome your feedback at [private.sector@hq.dhs.gov](mailto:private.sector@hq.dhs.gov).

From the borders to the boardroom, creating a safe, secure, and resilient nation where the American way of life can thrive will take every single one of us, both inside government and out. Simply put, homeland security is a shared responsibility and the private sector plays a key role. This document provides the resources necessary to fulfill that role.

The Department is committed to providing you with the assistance and support you require. You can contact my office any time with requests, comments, questions, issues or concerns at [private.sector@hq.dhs.gov](mailto:private.sector@hq.dhs.gov) or (202) 282-8484.

Sincerely,

Douglas A. Smith  
Assistant Secretary for the Private Sector

# Department-wide Resources

## *Civil Rights, Civil Liberties, and Privacy*

**Blue Campaign Toolkit** provides private sector stakeholders with a compiled list of training, resources, and actions you can take to combat human trafficking and raise awareness. It also provides links to anti-human trafficking resources available from other Federal Departments and Agencies. The Toolkit is available at [http://www.dhs.gov/files/programs/gc\\_1281551408757.shtm](http://www.dhs.gov/files/programs/gc_1281551408757.shtm).

**Blue Campaign to Combat Human Trafficking** is the Department of Homeland Security's first-of-its-kind initiative to coordinate and enhance the Department's anti-human trafficking efforts, led by a cross-component steering committee, which is chaired by the Senior Counselor to the Secretary. ICE is the primary agency within DHS that investigates human trafficking, and it runs a 24 hour hotline 1-866-DHS-2ICE (1-866-347-2423), for the public to report suspicious activity. The public can also call the National Human Trafficking Resource Center 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, indicator cards, shoe cards, and tear cards. For more information, see <http://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](http://www.dhs.gov/crcl).

**Community Roundtables** The DHS Office for Civil Rights and Civil Liberties (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, Middle Eastern, and Sikh communities with government representatives; other roundtables include immigrant communities and those with frequent DHS contacts. CRCL also conducts roundtables with young leaders of diverse communities. For more information please contact [CRCLOutreach@dhs.gov](mailto:CRCLOutreach@dhs.gov).

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

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

**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* (E.O. 12898), 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., DHS recently published an Environmental Justice Annual Implementation Report. For more information, or to view the report, see

<http://www.dhs.gov/xlibrary/assets/mgmt/dhs-fy2011-ej-ann-rpt.pdf>.

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

**Forced Labor Resources** The ICE Homeland Security Investigations (HSI) Office of International Affairs investigates allegations of forced labor in violation of the Tariff Act of 1930 (Title 19 USC §1307). To request more information or a copy of the A Forced Child Labor Advisory booklet and brochure, please contact: [ice.forcedlabor@ice.dhs.gov](mailto:ice.forcedlabor@ice.dhs.gov). When contacting ICE to report instances of forced labor, please provide as much detailed information and supporting documentation as possible, including the following: a full statement of the reasons for the belief that the product was produced by forced labor and that it may be or has been imported into the United States; a detailed description of the product; all pertinent facts known regarding the production of the product abroad. For the location of ICE foreign offices, please visit the ICE web site at <http://www.ice.gov>, click About Us, click International Affairs and select your country. ICE maintains a 24/7 hotline at (866) DHS-2-ICE (866-347-2423).

**Guide to Implementing Privacy** informs the public about how the DHS Privacy Office implements privacy at DHS. The guide provides an overview of the DHS Privacy Office's functions and transparency in day-to-day operations. For more information please visit [http://www.dhs.gov/xabout/structure/editorial\\_0338.shtm](http://www.dhs.gov/xabout/structure/editorial_0338.shtm).

**Guidance to Federal Financial Assistance Recipients Regarding Title VI Prohibition Against National Origin Discrimination Affecting Limited English Proficient Persons** On April 18, 2011 DHS, in

pursuance of Executive Order 13166 “Improving Access to Services for Persons with Limited English Proficiency” published this guidance to help those with limited English proficiency. For more information, see [http://www.dhs.gov/xabout/laws/gc\\_1277242893223.shtm](http://www.dhs.gov/xabout/laws/gc_1277242893223.shtm).

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

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

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

**Introduction to Arab American and Muslim American Cultures** is an hour-long training DVD 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 in the course of their duties. For more information, contact [crcl@dhs.gov](mailto:crcl@dhs.gov) or visit [www.dhs.gov/crcl](http://www.dhs.gov/crcl).

**Language Access** CRCL provides resources, guidance and technical assistance to recipients of financial

assistance from DHS to help ensure meaningful access to persons who are Limited English Proficient (LEP) as required by Title VI of the Civil Rights Act of 1964. CRCL is a member of the Federal Interagency Working Group on LEP, which hosts [www.LEP.gov](http://www.LEP.gov). Additionally, on February 28, 2011 DHS released its first-ever Department plan for providing meaningful access to homeland security programs to people with limited English proficiency. For more information, see <http://www.dhs.gov/files/publications/dhs-language-access-plan.shtm> or contact [crcl@dhs.gov](mailto:crcl@dhs.gov).

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

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

**No te Engañes (Don't be Fooled)** is the Customs and Border Protection (CBP) outreach campaign to raise awareness about human trafficking among potential migrants. For more information, please visit

[http://www.cbp.gov/xp/cgov/border\\_security/human\\_trafficking/](http://www.cbp.gov/xp/cgov/border_security/human_trafficking/) or contact Laurel Smith at [laurel.smith@dhs.gov](mailto:laurel.smith@dhs.gov) or 202-344-1582.

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

**Privacy Impact Assessments (PIAs)** are decision-making tools used to identify and mitigate privacy risks at the beginning of and throughout the development life cycle of a program or system. They help the public understand what personally identifiable information (PII) the Department is collecting, why it is being collected, and how it will be used, shared, accessed, and stored. All PIAs issued by DHS may be found here: [http://www.dhs.gov/files/publications/editorial\\_0511.shtm](http://www.dhs.gov/files/publications/editorial_0511.shtm).

**DHS Privacy Office** sustains privacy protections and the transparency of government operations while supporting the DHS mission. The DHS Privacy Office ensures DHS programs and operations comply with federal privacy laws and policies. Members of the public can contact the Privacy Office with concerns or complaints regarding their privacy. For more information, visit [www.dhs.gov/privacy](http://www.dhs.gov/privacy) or contact [privacy@dhs.gov](mailto:privacy@dhs.gov), (202) 235-0780.

**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 [http://www.dhs.gov/xfoia/editorial\\_0579.shtm](http://www.dhs.gov/xfoia/editorial_0579.shtm).

**Quarterly NGO Civil Rights / Civil Liberties Committee Meeting** CRCL hosts regular meetings

with representatives of over 20 civil society organizations primarily working on matters at the intersection of immigration and civil and human rights. Assisted by extensive grassroots networks, committee members articulate the concerns of organizations and communities across the country on these issues. The CRCL Officer meets quarterly with the committee to identify systemic and policy concerns relevant to CRCL. For more information please contact [CRCLOutreach@dhs.gov](mailto:CRCLOutreach@dhs.gov).

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

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

## Economic Analysis

**Computable General Equilibrium (CGE) Economic Analysis Model and Expanded Framework** is a state of the art methodology for performing economic

consequence analysis. For more information, see [http://create.usc.edu/research/Measuring Economic Resilience to Terrorism.pdf](http://create.usc.edu/research/Measuring_Economic_Resilience_to_Terrorism.pdf).

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

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

## Outreach and Engagement

**Building Resilience through Public-Private Partnerships Conference** Although online resources are valuable in their broad accessibility, sometimes face-to-face opportunities are the best way to fully engage people and encourage a productive exchange of ideas. The national conference on "Building Resilience through Public Private Partnerships" was

held in August 2011, and a second conference is planned for July 23-24, 2012 in Colorado Springs, Colorado. Combined in-person and virtual participation for the 2011 event reached close to 1,000 people nationwide. The conference was developed in collaboration with DHS HQ and USNORTHCOM and was co-hosted at the U.S. Chamber of Commerce and the American Red Cross Headquarters. The conference after action report is available on [www.fema.gov/privatesector](http://www.fema.gov/privatesector). USNORTHCOM is leading planning for the 2012 conference. Please contact [ncc.icgps.omb@northcom.mil](mailto:ncc.icgps.omb@northcom.mil) for more information.

**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 servicing 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 <http://www.cbp.gov/xp/cgov/toolbox/contacts/contacting/> or send an email to CBP's Industry Communication Liaison at the following email address: [robert.namejko@cbp.gov](mailto:robert.namejko@cbp.gov). Vendors seeking assistance of the Task Order Ombudsman should send an email to [francine.harris@dhs.gov](mailto:francine.harris@dhs.gov).

**Critical Manufacturing Working Groups** Critical Manufacturing SCC and 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 on a monthly basis and are posted on the CM HSIN site. For more information, see [http://www.dhs.gov/files/committees/gc\\_1277402\\_017258.shtm](http://www.dhs.gov/files/committees/gc_1277402_017258.shtm) or email [hsin.outreach@dhs.gov](mailto:hsin.outreach@dhs.gov).

### **Cross-Sector Supply Chain Working Group**

**(CSSCWG)** In December 2010, the Critical Manufacturing Sector co-sponsored the development of the Cross-Sector Supply Chain Working Group (CSSCWG), bringing together the 18 Critical Infrastructure Sectors to explore security issues surrounding the supply chain. One major goal of the working group is to review and share both the best practices and known gaps, in order to streamline the various supply chain efforts. For more information see [http://www.dhs.gov/files/committees/gc\\_1277402\\_017258.shtm](http://www.dhs.gov/files/committees/gc_1277402_017258.shtm) or email [NICCC@dhs.gov](mailto:NICCC@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 Coordinator (FC) (when designated by the Secretary of DHS for select events). The SEP provides the FC 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 resource needs are communicated across the agencies with responsibility for special event response. The SEP achieves this mission through collaboration with the interagency SEWG. For more information, please contact [OPS-SEWG@hq.dhs.gov](mailto: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](http://www.dhs.gov/fbci). For more information or to sign up to receive Information Updates, e-mail [Infobfci@dhs.gov](mailto:Infobfci@dhs.gov).

**DHS for a Day** This program was launched in 2010 to educate and engage the Department's private sector partners on the Homeland Security Enterprise. As of May 2012, the DHS Private Sector Office had coordinated nine events across the country focusing on issues ranging from supply chain security to emergency operations. For more information, see the [Blog @ DHS](#) or email [DHSforaDay@dhs.gov](mailto:DHSforaDay@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 <http://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, please e-mail [loanedexecutive@dhs.gov](mailto:loanedexecutive@dhs.gov).

**DHS Loaned Professor Program (via the Intergovernmental Personnel Act Mobility Program)** Spend your sabbatical at DHS! Contribute to our nation's security and gain in depth experience on homeland security issues ranging from cybersecurity to trade facilitation. For more information, please email [loanedexecutive@dhs.gov](mailto:loanedexecutive@dhs.gov).

The **DHS Private Sector Office (PSO)** serves as the primary advisor to the Secretary on all homeland security issues that impact the private sector, defined as businesses, academic institutions, trade associations, not-for-profits, and other non-governmental organizations. 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, see <http://www.dhs.gov/privatesector> or call 202-282-8484.

**FEMA Industry Liaison Program** is a point-of-entry for vendors seeking information on how to do business with FEMA during disasters and non-disaster periods of activity. The program coordinates vendor presentation meetings between vendors and FEMA program offices, establishes strategic relationships with vendor-supporting industry partners and stakeholders, coordinates Industry Days, conducts market research, responds to informal Congressional requests, and performs vendor analysis reporting. Vendors interested in doing business with FEMA should take the following steps: Register in the Central Contractor Registration (CCR) at [www.ccr.gov](http://www.ccr.gov), contact the FEMA Industry Liaison Program at <http://www.fema.gov/privatesector/industry/index.shtm>, or call the Industry Liaison Support Center at (202) 646-1895.

**FEMA Private Sector E-alerts** are periodic e-alerts providing timely information on topics of interest to private sector entities. To sign up for these and other alerts visit <http://www.fema.gov/help/getemail.shtm>.

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

**FEMA Think Tank** In 2012, FEMA launched a collaborative forum to engage our partners, promote innovation, and facilitate discussions in the field of emergency management. This forum is open to the whole community: state, local, and tribal governments, as well as all members of the public, including the private sector, the disability community, and volunteer community. The primary goal is to seek their input on how to improve the emergency management system, explore best practices and

generate new ideas. The FEMA Think Tank has two main components:

- **Online Forum:** Visitors can submit their own ideas, comment on others, and participate in conversations meant to generate creative solutions. The forum is open to anyone who wants to discuss a variety of emergency management issues, such as how we prepare for, respond to, recover from, or mitigate against all types of disasters, as well as ideas on how we can continue to integrate the whole community. (<http://fema.ideascale.com/>)
- **Monthly Conference Call Discussions:** Deputy Administrator Richard Serino held the first monthly conference call in January 2012, to discuss some of the real-life solutions and ideas that are generated by this online forum. These calls are open to the general public, with captioning for participants who are deaf or hard of hearing. The Deputy Administrator travels to a different location each month to personally meet with members of the emergency management community. To find out when the next call will be, see <http://www.fema.gov/thinktank/conferencerecalls.shtm>.

The **Homeland Security Advisory Council (HSAC)** provides advice and recommendations to the Secretary of Homeland Security on matters related to homeland security. The Council is comprised of 30 members selected by the Secretary that are leaders from State and local government, first responder communities, the private sector, and academia. The Council is an independent, bipartisan advisory board of leaders that recently produced reports on border security, countering violent extremism, community resilience, sustainability and efficiency, and the previous Homeland Security Advisory System. For more information or to apply to be a member, please visit [http://www.dhs.gov/files/committees/editorial\\_0331.shtm](http://www.dhs.gov/files/committees/editorial_0331.shtm) or contact at [hsac@dhs.gov](mailto:hsac@dhs.gov).

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

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

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

**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](https://service.govdelivery.com/service/subscribe.html?code=USDHS_99). For more information, contact [private.sector@dhs.gov](mailto:private.sector@dhs.gov) or (202) 282-8484.

**Private Sector for a Day** Following the success of the DHS for a Day program, the DHS Private Sector Office

launched this program in 2012 for partners from across the federal government to engage meaningfully with relevant experts in the private sector and to learn from private sector best practices on issues ranging from social media to cybersecurity. For more information, email [private.sector@dhs.gov](mailto:private.sector@dhs.gov).

**Private Sector Representative in the National Response Coordination Center** One of the most innovative programs at FEMA is one in which FEMA opens its doors to peers from the private sector for 90 days at a time. During this rotation, the Private Sector Representative is a special government employee representing the broad private sector (not just the home organization) and works side-by-side with us during normal operations and during disasters. The program started in 2011, and has included both Fortune 500 companies and small business. It is also open to academia and other segments of the private sector. Email [FEMA-PSR@fema.dhs.gov](mailto:FEMA-PSR@fema.dhs.gov).

**Private Sector Division/Office of External Affairs** FEMA established a Private Sector Division within the Office of External Affairs in October 2007. The division's purpose is 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. The division's vision is to establish and maintain a national reputation for effective support to our private sector stakeholders through credible, reliable and meaningful two-way communication. [Fema-private-sector@dhs.gov](mailto:Fema-private-sector@dhs.gov); [www.fema.gov/privatesector](http://www.fema.gov/privatesector)

**Regional and Disaster Private Sector Liaisons** In addition to the headquarters team, 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 private sector during steady state and disaster operations. During disasters, a reserve cadre of private sector specialists deploys to support Joint Field Office efforts, as part of ESF 15- External Affairs. For more information, please contact [fema-private-sector@dhs.gov](mailto:fema-private-sector@dhs.gov).

### **Sector-Specific Agency (SSA) for Communications**

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

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

## **Policy Guidance**

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

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

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

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

**IS-821 Critical Infrastructure Support Annex** is an independent study course that provides an introduction to the Critical Infrastructure Support

Annex to the National Response Framework. See <http://training.fema.gov/emiweb/is/is821.asp>, for more information, contact [IP\\_Education@hq.dhs.gov](mailto:IP_Education@hq.dhs.gov).

**IS-860.a National Infrastructure Protection Plan (NIPP)** is an Independent Study course that presents an overview of the NIPP. The NIPP provides the unifying structure for the integration of existing and future 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 <http://training.fema.gov/emiweb/is/is860a.asp> or contact [IP\\_Education@hq.dhs.gov](mailto:IP_Education@hq.dhs.gov).

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

**Guide to Critical Infrastructure Protection at the State, Regional, Local, Tribal, & Territorial Level(2008)** outlines the attributes, capabilities, needs, and processes that a state or local government entity should include in establishing its own critical infrastructure protection function that integrates with the National Infrastructure Protection Plan (NIPP) and accomplishes the desired local benefits. To download this document visit [http://www.dhs.gov/xlibrary/assets/nipp\\_srltt\\_guide.pdf](http://www.dhs.gov/xlibrary/assets/nipp_srltt_guide.pdf) or contact [NIPP@dhs.gov](mailto:NIPP@dhs.gov).

**Infrastructure Protection Report Series (IPRS)** is a comprehensive series of For Official Use Only (FOUO) reports containing detailed information for all 18 Critical Infrastructure and Key Resources (CIKR)

sectors focusing on infrastructure characteristics and common vulnerabilities, potential indicators of terrorist activity, potential threats, and associated protective measures. The IPRS is available to vetted private sector critical infrastructure owners and operators with a demonstrated need to know through the Homeland Security Information Network-Critical Sectors (HSIN-CS) (<https://cs.hsin.gov/>) online secure portal. For more information on the IPRS, critical infrastructure private sector owners and operators should contact [IPassessments@hq.dhs.gov](mailto:IPassessments@hq.dhs.gov).

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

**National Infrastructure Protection Plan (NIPP) 2009** provides the unifying structure for the integration of a wide range of efforts for the enhanced protection and resilience of the Nation's critical infrastructure into a single national program. For more information, see [http://www.dhs.gov/files/programs/editorial\\_0827.shtm](http://www.dhs.gov/files/programs/editorial_0827.shtm) or to request materials contact [NIPP@dhs.gov](mailto:NIPP@dhs.gov).

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

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

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

**Physical Security Criteria for Federal Facilities: An Interagency Security Committee Standard (FOUO)** This document is a new interim ISC standard. The standard establishes a baseline set of physical security measures to be applied to all federal facilities based on their designated facility security level. It also provides a framework for the customization of security measures to address unique risks faced at each facility. The interim standard will be used during a 24-month validation period to confirm the need and usability of this standard. For more information, please contact the NPPD/IP ISC at [ISC@dhs.gov](mailto:ISC@dhs.gov).

**Sector Annual Reports (FOUO)** The SSPs provide the means by which the NIPP is implemented across all critical infrastructure sectors. Each Sector-Specific Agency is responsible for developing and implementing an SSP through a coordinated effort involving their public and private sector critical infrastructure partners. Collaborating with government and private sector to develop, update, and maintain Sector Annual Reports for the Chemical, Commercial Facilities, Critical Manufacturing, Dams,

Emergency Services, and Nuclear Sectors. For more information please contact [SOPDExecSec@dhs.gov](mailto:SOPDExecSec@dhs.gov)

**Sector-Specific Plans** SSPs support the National Infrastructure Protection Plan (NIPP) by establishing a coordinated approach to national priorities, goals, and requirements for critical infrastructure protection. Each SSP provides the means by which the NIPP is implemented for each sector, as well as a national framework to address the sector's unique characteristics and risk landscape. Copies of the 2010 SSPs that are not marked FOUO can be downloaded at: [http://www.dhs.gov/files/programs/gc\\_117986619\\_7607.shtm](http://www.dhs.gov/files/programs/gc_117986619_7607.shtm).

**State and Local Implementation Snapshot** In accordance with the National Infrastructure Protection Plan (NIPP), as well as the requirements identified in the Homeland Security Grant Program, State and tribal governments are responsible for developing, implementing, and sustaining a statewide/regional critical infrastructure protection program. The processes necessary to implement the NIPP risk management framework at the state and/or regional level, including urban areas, should become a component of the state's overarching homeland security program. This two-page snapshot presents information on a variety of resources available to support State/local and tribal critical infrastructure protection efforts. For more information, see [http://www.dhs.gov/xlibrary/assets/nipp\\_state\\_local\\_snapshot.pdf](http://www.dhs.gov/xlibrary/assets/nipp_state_local_snapshot.pdf).

## 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 the purpose of 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.

<http://apfs.dhs.gov/>

**CBP Laboratories and Scientific Services** coordinates technical and scientific support to all CBP trade and border protection activities. For more information, visit

[http://www.cbp.gov/xp/cgov/trade/automated/labs\\_scientific\\_svcs/](http://www.cbp.gov/xp/cgov/trade/automated/labs_scientific_svcs/).

**Cooperative Research and Development Agreements (CRADAs)** are part of the national Technology

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

**Commercialization Office** develops and executes programs and processes that identify, evaluate, and commercialize technologies into products or services that meet the detailed operational requirements of DHS stakeholders. The Commercialization Office also spearheads DHS Science and Technology Directorate outreach efforts to inform the private sector on doing business with DHS. For more information, see [http://www.dhs.gov/xabout/structure/gc\\_1234194\\_479267.shtm](http://www.dhs.gov/xabout/structure/gc_1234194_479267.shtm). Contact: [SandT\\_Commercialization@hq.dhs.gov](mailto:SandT_Commercialization@hq.dhs.gov), (202) 254-6749.

### **Defense Technology Experimental Research**

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

**DHS Technology Transfer Program** promotes the transfer and/or exchange of technology with industry, state and local governments, academia, and other federal agencies. The technologies developed and evaluated within DHS can have potential commercial applications and dramatically enhance the competitiveness of individual small businesses as well as expanding areas of cooperation for non-federal partners. For more information, visit [http://www.dhs.gov/xabout/structure/gc\\_1264538\\_499667.shtm](http://www.dhs.gov/xabout/structure/gc_1264538_499667.shtm).

### **DHS Small Business Innovation Research (SBIR)**

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

**FutureTECH™** targets critical research/innovation focus areas to communicate to the private sector and national labs the long-term needs of the Department. For more information, see [http://www.dhs.gov/files/programs/gc\\_124205879\\_4349.shtm](http://www.dhs.gov/files/programs/gc_124205879_4349.shtm) or contact

[SandT\\_Commercialization@hq.dhs.gov](mailto:SandT_Commercialization@hq.dhs.gov), (202) 254-6749.

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

### **Long Range Broad Agency Announcement (LRBAA)**

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

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

### **National Urban Security Technology Laboratory**

**(NUSTL)** tests, evaluates, and analyzes homeland security capabilities while serving as a technical authority to first responder, state, and local entities.

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

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

**Project 25 Compliance Assessment Program (P25 CAP)** was established, in coordination with the National Institute of Standards and Technology (NIST), to provide a process for ensuring that equipment complies with P25 standards, meets performance requirements, and is capable of interoperating across manufacturers. P25 CAP allows emergency responders to confidently purchase and use P25-compliant products. For more information, see [http://www.pscr.gov/projects/lmr/p25\\_cap/p25\\_ca.php](http://www.pscr.gov/projects/lmr/p25_cap/p25_ca.php) or contact [P25CAP@dhs.gov](mailto:P25CAP@dhs.gov).

**Research and Standards Integration Program (RSI)** interfaces with public and private sector organizations to advance the future state of cybersecurity through Research and Development (R&D) and standards for information and communications technology. RSI seeks input from academic and industry researchers to determine if their R&D projects map to CS&C R&D

requirements, particularly to identify relevant federally funded research in areas such as visualization for cybersecurity, enterprise-level situational awareness, and analytic frameworks. For more information, contact [RSI@hq.dhs.gov](mailto: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, [SandT.Research@dhs.gov](mailto:SandT.Research@dhs.gov), and (202) 254-6068.

**SECURE™ Program** leverages the experience and resources of the private sector to develop fully deployable products/services based on Department generated and vetted, detailed commercialization-based operational requirements documents and a conservative estimate of the potential available market of Department stakeholders. For more information, see [http://www.dhs.gov/files/programs/gc\\_121199662\\_0526.shtm](http://www.dhs.gov/files/programs/gc_121199662_0526.shtm), or contact [sandt\\_commercialization@hq.dhs.gov](mailto:sandt_commercialization@hq.dhs.gov), (202) 254-6749.

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

see [www.SAFETYAct.gov](http://www.SAFETYAct.gov) or contact [SAFETYActHelpDesk@dhs.gov](mailto:SAFETYActHelpDesk@dhs.gov), (866) 788-9318.

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

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

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

including an independent and objective certification/qualification process for technologies. For more information, contact [tsinfo@dhs.gov](mailto:tsinfo@dhs.gov).

## Protecting Against Fraud & Counterfeiting

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

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

**Commercial Fraud** ICE Homeland Security Investigations (HSI) investigates commercial fraud, including false statements and deceptive business practices. The ICE HSI Commercial Fraud Programs Unit, which is led by the IPR Center, prioritizes health and safety violations, U.S. economic interests, and duty collection. For more information, see <http://www.iprcenter.gov/reports/fact-sheets/commercial-fraud/view>.

**eInformation Network** The Secret Service eInformation Network is available – for free – to authorized law enforcement officers, financial institution investigators, academic partners, and

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

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

**Financial Crimes Task Forces (FCTF)** combines the resources of the Secret Service, state and local law enforcement, and the financial industry to combat financial crimes. The technological advance of domestic and transnational criminals allows new avenues to exploit financial institutions, thus making internationally-based criminal enterprises even more problematic for law enforcement. The most effective means of combating organized criminal elements, both in the U.S. and abroad, is through the use of Financial Crimes Task Forces. The multi-agency components are well suited to conduct complex, in-

depth, multi-jurisdictional investigations. For more information contact your local Secret Service field office at [www.secretservice.gov/field\\_offices.shtml](http://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 [http://www.cbp.gov/linkhandler/cgov/trade/priority\\_trade/ipr/legal/ipr\\_guide.ctt/ipr\\_guide.pdf](http://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)** ICE recognizes that the private sector represents America's first line of defense against money laundering. With IFPCU, ICE Homeland Security Investigations reaches out to the U.S. business community, along with state and federal agencies to combat financial and trade crimes. IFPCU identifies and eliminates vulnerabilities within the U.S. financial, trade and transportation sectors--vulnerabilities that criminal and terrorist organizations could exploit to finance their illicit operations and avoid being detected by law enforcement. The IFPCU publishes the Cornerstone Report, a quarterly newsletter. This report provides current trends and financial crimes identified by law enforcement and the private sector. To subscribe to the Cornerstone Report, or for more information, see [www.ice.gov/cornerstone](http://www.ice.gov/cornerstone) or call (866) DHS-2-ICE (866-347-2423).

**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 <http://www.ice.gov/exec/forms/hsi-tips/tips.asp>

**Intellectual Property Rights (IPR) Fact Sheet** U.S. Customs and Border Protection (CBP) enforces IPR, most visibly by seizing products that infringe IPR such as trademarks, copyrights, and patents. 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 [http://www.cbp.gov/linkhandler/cgov/newsroom/fact\\_sheets/trade/ipr\\_fact\\_sheet.ctt/ipr\\_fact\\_sheet.pdf](http://www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/trade/ipr_fact_sheet.ctt/ipr_fact_sheet.pdf)

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

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

**Intellectual Property Rights (IPR) Enforcement: A Priority Trade Issue** The trade in counterfeit and pirated goods threatens America's innovation economy, the competitiveness of our businesses, the livelihoods of U.S. workers, national security, and the health and safety of consumers. The trade in these illegitimate goods is associated with smuggling and other criminal activities, and often funds criminal enterprises. For more information, visit [www.cbp.gov/ipr](http://www.cbp.gov/ipr).

**Intellectual Property Rights (IPR) e-Recordation and IPR Search** The first step in obtaining IPR protection by CBP is to record validly registered trademarks and copyrights with CBP through the Intellectual Property Rights e-Recordation (IPRR) online system. The CBP on-line recordation allows intellectual property owners to electronically record their trademarks and copyrights with CBP, and makes IPR recordation information readily available to CBP personnel, facilitating IPR seizures by CBP. CBP uses recordation information to actively monitor shipments and prevent the importation or exportation of infringing goods. For more information, see <http://iprs.cbp.gov/> or contact [hqiprbranch@dhs.gov](mailto:hqiprbranch@dhs.gov) (202) 325-0020.

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

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

**IPR Product Identification Guide** Organizations that are concerned about intellectual property violations at America's borders may submit a Product Identification Guide that will easily allow CBP Officers to determine which products are genuine and which are counterfeit. For more information, see [http://www.cbp.gov/xp/cgov/trade/priority\\_trade/ipr/legal/training\\_guide/](http://www.cbp.gov/xp/cgov/trade/priority_trade/ipr/legal/training_guide/)

**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](mailto:IPRCenter@dhs.gov), visit [www.iprcenter.gov](http://www.iprcenter.gov), or call 866-IPR-2060. For more information on the IPR center, see <http://www.iprcenter.gov/reports/fact-sheets/national-intellectual-property-rights-ipr-coordination-center-ipr-investigations>.

**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](mailto:IBFU-ICE-HQ@DHS.GOV).

**Operation Guardian** is a multi-agency effort to combat the increasing importation of substandard, tainted, and counterfeit products that pose a health and safety risk to consumers. The identification of these commodities has led to the successful detention and seizure of numerous containers of hazardous products. For more information, visit <http://www.iprcenter.gov/reports/fact-sheets/Operation%20Guardian%20Fact%20Sheet%20FINAL%20-%20IPR%20DIRECTOR%20APPROVAL.pdf/view>.

**Operation In Our Sites** specifically targets websites and their operators that distribute counterfeit and pirated items over the Internet, including counterfeit pharmaceuticals and pirated movies, television shows, music, software, electronics, and other merchandise, as well as products that threaten public health and safety. For more information, visit <http://www.ice.gov/doclib/news/library/factsheets/pdf/operation-in-our-sites.pdf>.

**Report an IPR Violation** In furtherance of the U.S. Government's IPR enforcement efforts, the IPR Center

continues to encourage the general public, industry, trade associations, law enforcement, and government agencies to report violations of intellectual property rights. To better facilitate IP theft reporting, the IPR Center created an “IP Theft Button.” As a result, anyone in the world with Internet access has the capability to report an IPR violation and provide information directly to the IPR Center for investigative consideration. If a company or individual has specific information concerning IP theft, they can send an email to [IPRCenter@dhs.gov](mailto:IPRCenter@dhs.gov), visit [www.iprcenter.gov](http://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.

<http://www.iprcenter.gov/reports/Reporting%20Allergations%20of%20Intellectual%20Property%20Theft%20Brochure.pdf/view>

## 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 <http://blog.dhs.gov>.

**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 <http://cgmarinesafety.blogspot.com>, <http://harborsafetycommittee.blogspot.com/>, [www.uscgnews.com](http://www.uscgnews.com), or [www.twitter.com/uscoastguard](http://www.twitter.com/uscoastguard).

**CRCL’s Facebook Page** allows our Office to instantly connect with the public and share information about our work supporting the Department to secure the nation while preserving individual liberty, fairness, and equality under the law. Through our Facebook page, we share important information about DHS programs and policies and engage with our “friends”

to receive feedback, and learn about civil rights and civil liberties issues occurring in communities throughout the country. [“Like” our page](#), and start a conversation.

**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 [http://www.dhs.gov/xabout/gc\\_1238684422624.shtml](http://www.dhs.gov/xabout/gc_1238684422624.shtml).

**USCIS Social Media** tools both provide information to and engage in discussions with the public. These tools include The Beacon – The official blog of USCIS -at [www.uscis.gov/blog](http://www.uscis.gov/blog); Twitter channels in both English [www.twitter.com/uscis](http://www.twitter.com/uscis) and Spanish [www.twitter.com/uscis\\_es](http://www.twitter.com/uscis_es); and a YouTube channel for hosting video content [www.youtube.com/uscis](http://www.youtube.com/uscis)

**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](http://www.fema.gov/privatesector).

# Preventing Terrorism and Enhancing Security

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

## Aviation Security

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

**AIRBUST Program** provides the general public and aviation community with a forum to share information on suspicious small aircraft. An AIRBUST poster and pocket-sized laminated card display the phone number for reporting suspicious activity or low-flying aircraft, 1-866-AIRBUST (1-866-247-2878). This number rings directly to the CBP Air and Marine Operations Center (AMOC) operations floor. The two-sided laminated card displays drawings of single-and twin-engine aircraft often used to transport contraband and lists helpful information to include when calling. The AIRBUST poster is an 8.5x11" poster with the 1-866-AIRBUST (1-866-247-2878) phone number. It also lists four general items of interest that can tip off a general aviation airport employee or law enforcement official that a particular aircraft or pilot may be involved in illicit activity. For more information, call 951-656-8000.

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

**Air Cargo Watch Program** involves all aspects of the supply chain reporting suspicious activity. TSA is collaborating with industry partners to increase security domain awareness to detect, deter, and report security threats. Air Cargo Watch materials include a presentation, posters and a two-page guide, to encourage increased attention to potential security threats among several audiences. TSA encourages the display of posters and guides in public view to better attain its goal of maximizing security awareness along the entire air cargo supply chain. For more information, see [http://www.tsa.gov/what\\_we\\_do/layers/aircargo/watch.shtm](http://www.tsa.gov/what_we_do/layers/aircargo/watch.shtm).

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

**Airspace Waivers** The Office of Airspace Waivers manages the process and assists with the review of general aviation aircraft operators who request to enter areas of restricted airspace. For applications for aircraft operating into, out of, within or overflying the United States, the waiver review process includes an evaluation of the aircraft, crew, passengers, and purpose of flight. The office then adjudicates the application and provides a recommendation of approval or denial to the FAA System Operations Security. For more information, see [http://www.tsa.gov/what\\_we\\_do/tsnm/general\\_aviation/programs\\_aw.shtm#overview](http://www.tsa.gov/what_we_do/tsnm/general_aviation/programs_aw.shtm#overview) or contact (571) 227-2071.

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

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

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

**General Aviation Maryland Three Program** allows properly vetted private pilots to fly to, from, or between the three general aviation airports closest to the National Capital Region. These airports are collectively known as the "Maryland Three" airports, and include College Park Airport (CGS), Potomac Airfield (VKX) and Hyde Executive Field (W32). These airports are all within the Washington, DC Air Defense Identification Zone and the Washington, D.C. Flight Restricted Zone. For more information, see [http://www.tsa.gov/what\\_we\\_do/tsnm/general\\_aviation/programs\\_sp.shtm#maryland](http://www.tsa.gov/what_we_do/tsnm/general_aviation/programs_sp.shtm#maryland) or contact [MDThree@dhs.gov](mailto:MDThree@dhs.gov).

**General Aviation Security Guidelines** are for security enhancements at the nation's privately and publicly owned and operated general aviation (GA) landing facilities. The document constitutes a set of federally endorsed guidelines for enhancing airport security at GA facilities throughout the nation. It is intended to provide GA airport owners, operators, and users with guidelines and recommendations that address aviation security concepts, technology, and enhancements. For more information, visit [http://www.tsa.gov/what\\_we\\_do/tsnm/general\\_aviation/airport\\_security\\_guidelines.shtm](http://www.tsa.gov/what_we_do/tsnm/general_aviation/airport_security_guidelines.shtm).

**Global Supply Chain Risk Management (GSCRM) Program** provides recommendations to standardize and implement risk management processes for acquiring information and communications technologies (ICT) for the federal government, and

processes to reduce the threat of attacks to federal ICT through the supply chain. Your organization can help with this initiative by applying sound security procedures and executing due diligence to provide integrity and assurance through the vendor supply chain. For more information, visit [http://www.dhs.gov/files/programs/gc\\_1234200709381.shtm](http://www.dhs.gov/files/programs/gc_1234200709381.shtm) or contact the Global Supply Chain Program at [Kurt.Seidling@hq.dhs.gov](mailto:Kurt.Seidling@hq.dhs.gov).

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

**Private Aircraft Travel Entry Programs** The Advance Information on Private Aircraft Arriving and Departing the United States Final Rule requires that pilots of private aircraft submit advance notice and manifest data on all persons traveling on board. Required information must be submitted to CBP via an approved electronic data interchange system no later than 60 minutes prior to departure. For more information, please visit <http://www.cbp.gov/xp/cgov/travel/>. For additional questions or concerns, please contact CBP via e-mail at [Private.Aircraft.Support@dhs.gov](mailto:Private.Aircraft.Support@dhs.gov).

**Recommended General Aviation Security Action Items for General Aviation Aircraft Operators and Recommended Security Action Items for Fixed Base Operators** are measures that aircraft operators and fixed base operators should consider when they develop, implement or revise security plans or other efforts to enhance security. For more information, see [http://www.tsa.gov/what\\_we\\_do/tsnm/general\\_aviation/security.shtm](http://www.tsa.gov/what_we_do/tsnm/general_aviation/security.shtm).

**Secure Flight** enhances the security of domestic and international commercial air travel, while also

enhancing the travel experience for passengers, through the use of improved, uniform watchlist matching performed by TSA agents. Secure Flight also incorporates an expedited and integrated redress process for travelers who think they have been misidentified or have experienced difficulties in their air travel. Resources available for aviation stakeholders include a communications toolkit, brochure, privacy information, signage, and an informational video. For more information, visit [http://www.tsa.gov/what\\_we\\_do/layers/secureflight/index.shtm](http://www.tsa.gov/what_we_do/layers/secureflight/index.shtm), or contact the TSA Contact Center, (866) 289-9673.

**User's Guide on Security Seals for Domestic Cargo** provides information on the types of security seals available for use in securing and controlling containers, doors, and equipment. While this guide is not intended as a precise procedure for developing a comprehensive seal control program, 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/LOCS/PDF\\_FILES/sealguid.pdf](https://portal.navfac.navy.mil/portal/page/portal/NAVFAC/NAVFAC_WW_PP/NAVFAC_NFESC_PP/LOCS/PDF_FILES/sealguid.pdf).

## Bombing Prevention

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

To request materials or additional information, contact the DHS Office for Bombing Prevention at [OBP@dhs.gov](mailto:OBP@dhs.gov).

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

**Improvised Explosive Device (IED) Awareness / Bomb Threat Management Workshop** is a four-hour Workshop which improves participants' ability to manage improvised explosive device (IED) threats by outlining specific safety precautions associated with explosive incidents and bomb threats. The Workshop reinforces an integrated combination of planning, training, exercises, and equipment acquisition in order to maximize available resources. Key public and private sector representatives knowledgeable in regional efforts should attend. This Workshop is designed to accommodate 50 participants. To request training, contact your State Homeland Security Advisor; see [http://www.dhs.gov/xgovt/editorial\\_0291.shtm](http://www.dhs.gov/xgovt/editorial_0291.shtm) for a current list.

**Improvised Explosive Device (IED) Counterterrorism Workshop** is a four to eight-hour awareness level Workshop designed to enhance the knowledge of state and local law enforcement and public/private sector stakeholders by providing exposure to key elements of the IED threat, surveillance detection methods and soft target awareness. The Workshop illustrates baseline awareness and prevention actions that reduce vulnerabilities to counter the threat along with

collaborating information sharing resources to improve preparedness. This designed approach better enables the owners and operators of critical infrastructure to deter, prevent, detect, protect against, and respond to the potential use of explosives in the United States. This Workshop is designed to accommodate 125 to 250 participants. To request training, contact your State Homeland Security Advisor; see [http://www.dhs.gov/xgovt/editorial\\_0291.shtm](http://www.dhs.gov/xgovt/editorial_0291.shtm) for a current list.

**Improvised Explosive Device (IED) Recognition and Detection for Railroad Industry Employees Training (CD)** is an eight-hour Workshop which enhances participants' knowledge of improvised explosive device (IED) awareness, prevention measures, and planning protocols by outlining specific search techniques that reduce vulnerability and mitigate the risk of potential IED attacks. The Workshop culminates in a practical application of skills during which participants demonstrate these search techniques while working together as a team. Law enforcement and private sector security personnel responsible for bomb threat management planning and response should attend. This Workshop is designed to accommodate 40 participants. To request training, contact your State Homeland Security Advisor; see [http://www.dhs.gov/xgovt/editorial\\_0291.shtm](http://www.dhs.gov/xgovt/editorial_0291.shtm) for a current list.

**Improvised Explosive Device (IED) Search Procedures Workshop** is an eight-hour Workshop which enhances participants' knowledge of improvised explosive device (IED) awareness, prevention measures, and planning protocols by outlining specific search techniques that reduce vulnerability and mitigate the risk of terrorist IED attacks. The Workshop culminates in a practical application of skills during which participants demonstrate these search techniques while working together as a team. Law enforcement and private sector security personnel responsible for bomb threat management planning and response should attend.

This Workshop is designed to accommodate 40 participants. To request training, contact your State Homeland Security Advisor; see [http://www.dhs.gov/xgovt/editorial\\_0291.shtm](http://www.dhs.gov/xgovt/editorial_0291.shtm) for a current list.

**Improvised Explosive Device (IED) Threat Awareness and Detection)** The Office of Infrastructure Protection's Office for Bombing Prevention and the Commercial Facilities Sector-Specific Agency developed the first in a series of Web-based trainings, *Threat Awareness & Response for Sporting Events and Public Venues*, to be released in three 20-minute modules. The first Webinar, IED Threat Awareness and Detection, focuses on identifying Improvised Explosive Devices (IEDs). The training provides awareness-level information for staff, management, and security to recognize, report, and react to unusual activities and threats in a timely manner. For more information, please contact the NPPD/IP Commercial Facilities SSA at [CFSTeam@dhs.gov](mailto:CFSTeam@dhs.gov).

**Multi-Jurisdiction Improvised Explosive Device (IED) Security Plan (MJIEDSP)** assists multi-jurisdiction areas in developing a detailed IED security plan that integrates the assets and capabilities of multiple jurisdictions and emergency service sectors. To request additional information, contact the DHS Office for Bombing Prevention at [OBP@dhs.gov](mailto:OBP@dhs.gov).

**Protective Measures Course** is a two-day course designed to provide executive and employee level personnel in the public/private sector with the knowledge to identify the appropriate protective measures for their unique sector. The course focuses on teaching the participants the threat analysis process, terrorist methodology and planning cycle, available protective measures, and determining which protective measures to employ. This course is designed to accommodate 75 participants. To request training, contact your State Homeland Security Advisor; see [http://www.dhs.gov/xgovt/editorial\\_0291.shtm](http://www.dhs.gov/xgovt/editorial_0291.shtm) for a current list.

**Surveillance Detection for Law Enforcement and Security Professionals** is a three-day course designed for law enforcement and private sector security professionals that provides participants with the knowledge, skills, and abilities to detect hostile surveillance conducted against critical infrastructure. The course, consisting of five lectures and three exercises, increases awareness of terrorist tactics and attack history and illustrates the means and methods used to detect surveillance and identify suspicious behavior. This course is designed to accommodate 25 participants. To request training, contact your State Homeland Security Advisor; see [http://www.dhs.gov/xgovt/editorial\\_0291.shtm](http://www.dhs.gov/xgovt/editorial_0291.shtm) for a current list.

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

## Chemical Security

**Chemical Facility Anti-Terrorism Standards (CFATS) Chemical Facility Security Tip Line** Individuals who would like to report a possible security concern involving the CFATS regulation at their facility or at another facility may contact the CFATS Chemical Facility Security Tip Line. For more information, see [www.dhs.gov/chemicalsecurity](http://www.dhs.gov/chemicalsecurity) or contact (877) FYI-4-DHS (1-877-394-4347). To report a potential security incident that has already occurred, call the National Infrastructure Coordinating Center at (202) 282-9201.

**Chemical Facility Anti-Terrorism Standards (CFATS) Frequently Asked Questions** assist facilities in complying with the CFATS regulation. The FAQs are searchable and categorized to further benefit the user and can be found at <http://csat-help.dhs.gov/pls/apex/f?p=100:1:7096251139780888>. For more information, contact the CFATS Help Desk at [CSAT@dhs.gov](mailto:CSAT@dhs.gov) (866) 323-2957.

**Chemical Facility Anti-Terrorism Standards (CFATS) Presentations** are used by the Infrastructure Security Compliance Division (ISCD) in discussions with the chemical industry and those interested in chemical security. If interested in a live presentation about CFATS by ISCD personnel, or to find more information about such presentations see [http://www.dhs.gov/files/programs/gc\\_1224766914427.shtm](http://www.dhs.gov/files/programs/gc_1224766914427.shtm) or contact the CFATS at [cfats@dhs.gov](mailto:cfats@dhs.gov), (866) 323-2957.

**Chemical Facility Anti-Terrorism Standards (CFATS) Risk-Based Performance Standards (RBPS)** To assist high-risk chemical facilities subject to CFATS in selecting and implementing appropriate protective measures and practices to meet the DHS-defined RBPSs, ISCD has developed a Risk-Based Performance Standards Guidance document. This document can be found at [http://www.dhs.gov/xlibrary/assets/chemsec\\_cfats\\_riskbased\\_performance\\_standards.pdf](http://www.dhs.gov/xlibrary/assets/chemsec_cfats_riskbased_performance_standards.pdf). For more information, contact the CFATS Help Desk at [CSAT@dhs.gov](mailto: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](mailto:ChemicalSector@hq.dhs.gov).

**Chemical Security Analysis Center (CSAC)** provides a scientific basis for the awareness of chemical threats

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

**Chemical Security Assessment Tool (CSAT)** is an online tool developed by the Infrastructure Security Compliance Division (ISCD) to streamline the facility submission and subsequent DHS analysis and interpretation of critical information used to: preliminarily determine facility risk; assess high-risk facility vulnerability; describe security measures at high risk sites; and, ultimately track compliance with the CFATS program. CSAT is a secure information portal that includes applications and user guides for completing the User Registration, Top-Screen, Security Vulnerability Assessment, and Site Security Plan. For more information, see [http://www.dhs.gov/files/programs/gc\\_1169501486197.shtm](http://www.dhs.gov/files/programs/gc_1169501486197.shtm) or contact the CFATS Help Desk at [CSAT@dhs.gov](mailto:CSAT@dhs.gov). (866) 323-2957.

**Chemical Security Compliance Assistance Visit (CAV) Requests** are provided by the Infrastructure Security Compliance Division (ISCD) upon request by Chemical Facility Anti-Terrorism Standards (CFATS)-covered facilities. CAVs are designed to provide in-depth knowledge of and assistance to comply with CFATS. For more information, see [http://www.dhs.gov/files/programs/gc\\_1247235870769.shtm](http://www.dhs.gov/files/programs/gc_1247235870769.shtm) or contact [CFATS@hq.dhs.gov](mailto:CFATS@hq.dhs.gov).

**Chemical Security Summit** The NPPD/IP's Chemical Sector Specific Agency (SSA) co-hosts the annual Chemical Sector Security Summit with the Chemical Sector Coordinating Council (SCC). The Summit consists of workshops, presentations, and discussions covering current security regulations, industry best practices, and tools for the Chemical Sector. Designed for industry professionals throughout the Chemical Sector, there is also broad representation from the chemical stakeholder community, including senior DHS officials, congressional staff, and senior government officials. Topics covered at the Summits include: an overview of Chemical Facility Anti-Terrorism Standards (CFATS); harmonization of the various chemical regulations; cyber security, state and local issues, and transportation security. Summits also include pre-Summit Demonstrations and post-Summit workshops. For more details on the Summit, please visit [www.dhs.gov/chemicalsecuritysummit](http://www.dhs.gov/chemicalsecuritysummit) or contact the NPPD/IP Chemical SSA at [ChemicalSector@hq.dhs.gov](mailto:ChemicalSector@hq.dhs.gov).

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

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

**Chemical Sector Industrial Control Systems (ICS) Security Resource DVD** The chemical industry, in partnership with DHS, has collected a wealth of cybersecurity information to assist owners and

operators in addressing ICS security. The DVD contains a wide-range of useful information, including: ICS training resources; existing standards; reporting guidelines; cybersecurity tabletop exercises; and the National Cyber Security Division's Cyber Security Evaluation Tool. The DVD is available for free upon request. For more information or to obtain a copy of the DVD, please contact the NPPD/IP Chemical SSA at [ChemicalSector@hq.dhs.gov](mailto:ChemicalSector@hq.dhs.gov).

**Security Awareness Guide** The purpose of this document is to assist owners and operators in their efforts to improve security at their chemical facility and to provide information on the security threat presented by explosive devices and cyber vulnerabilities. For more information, please contact the NPPD/IP Chemical SSA at [ChemicalSector@hq.dhs.gov](mailto:ChemicalSector@hq.dhs.gov).

**Chemical Sector Training Resources Guide** The guide contains a list of free or low-cost training, web-based classes, seminars, and documents that are routinely available through one of several component agencies within DHS. The list was compiled to assist facility security officers to train their employees on industry best practices, physical and cybersecurity awareness, and emergency management and response. For more information, please contact the NPPD/IP Chemical SSA at [ChemicalSector@hq.dhs.gov](mailto:ChemicalSector@hq.dhs.gov).

**Chemical-Terrorism Vulnerability Information (CVI)** is the information protection regime authorized by Section 550 of Public Law 109-295 to protect, from inappropriate public disclosure, any information developed or submitted pursuant to Section 550. This includes information that is developed and/or submitted to DHS pursuant to the Chemical Facility Anti-Terrorism Standards (CFATS) regulation which implements Section 550. See [http://www.dhs.gov/files/programs/gc\\_1181835547413.shtm](http://www.dhs.gov/files/programs/gc_1181835547413.shtm). For more information, contact the CFATS Help Desk at [CSAT@dhs.gov](mailto:CSAT@dhs.gov) (866) 323-2957.

**Infrastructure Protection Sector-Specific Tabletop Exercise Program (IP-SSTEP), Chemical Sector**

**Tabletop Exercise (TTX)** The IP-SSTEP Chemical Sector TTX is an unclassified and adaptable exercise developed to create an opportunity for public and private critical infrastructure stakeholders and their public safety partners to address gaps, threats, issues, and concerns identified in previous exercises and their after-action processes. The TTX allows participants an opportunity to gain an understanding of issues faced prior to, during, and after a terrorist threat/attack and the needed coordination with other entities, both private and government, regarding their facility. It also contains everything needed for a company or facility to conduct a Homeland Security Exercise and Evaluation Program (HSEEP) compliant TTX. For more information, please contact the NPPD/IP Chemical SSA at [ChemicalSector@hq.dhs.gov](mailto:ChemicalSector@hq.dhs.gov).

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

**Security Seminar & Exercise Series for Chemical Industry Stakeholders** This is a collaborative effort between the DHS Chemical SSA and industry stakeholders such as state chemical industry councils, state homeland security offices, industry trade associations and state emergency management agencies. The intent of the program is to foster communication between facilities and their local emergency response teams by encouraging representatives to share their insight, knowledge, and experiences during a facilitated tabletop exercise. The exercise is catered towards the specific interests of the organizing entity and can include a wide-variety of topics and security scenarios such as an active shooter, a hostage situation, a suspicious package, or a Vehicle Borne improvised explosive device (VBIED). For

more information or to obtain a list of scheduled events, please contact the NPPD/IP Chemical SSA at [ChemicalSector@hq.dhs.gov](mailto:ChemicalSector@hq.dhs.gov).

**Voluntary Chemical Assessment Tool (VCAT)** VCAT is a secure, web-based application and self-assessment tool originally designed for use by the chemical industry. The tool allows owners and operators to identify their facility's current risk level using an all-hazards approach. VCAT facilitates a cost-benefit analysis by allowing users to select the best combination of physical security countermeasures and mitigation strategies to reduce overall risk. For more information, please contact the NPPD/IP Chemical SSA at [ChemicalSector@hq.dhs.gov](mailto:ChemicalSector@hq.dhs.gov).

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

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

## Critical Infrastructure – Multiple Sectors

**Automated Critical Asset Management System (ACAMS) Web-Based Training** provides federal, state, local first responders, emergency managers, and Homeland Security officials with training on the use and functionality of the ACAMS tool. Completion of training is required in order to access information

within ACAMS. For more information, contact [Traininghelp@hq.dhs.gov](mailto:Traininghelp@hq.dhs.gov).

**Critical Infrastructure Asset Protection Technical Assistance Program (CAPTAP)** is a weeklong course designed to assist state and local law enforcement, first responders, emergency managers, and other homeland security officials understand the steps necessary to develop and implement a comprehensive CIKR protection program in their respective jurisdiction. The course includes the processes, methodologies, and resources necessary to identify, assess, prioritize, and protect CIKR assets, as well as those capabilities necessary to prevent and respond to incidents, should they occur. Through a partnership with the National Guard Bureau (NGB), the U.S. Army Research, Development and Engineering Command (RDECOM), and the DHS Office of Infrastructure Protection (IP) Infrastructure Information Collection Division (IICD), this service also provides web-based and instructor-led training on Protected Critical Infrastructure Information (PCII) and the use of the Automated Critical Asset Management System (ACAMS) and Integrated mapping and geospatial tool. For more information, see [www.dhs.gov/files/programs/gc\\_1195679577314.shtm](http://www.dhs.gov/files/programs/gc_1195679577314.shtm) or contact [TrainingHelp@hq.dhs.gov](mailto:TrainingHelp@hq.dhs.gov).

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

**Critical Infrastructure Resource Center** is an online tool designed to build awareness and understanding of the scope and efforts of all of the 18 critical infrastructure sectors. Each sector page provides Sector goals, priorities, protective programs, and initiatives, and other resources, as reflected in the latest Sector-Specific Plans and Sector Web pages. To access the Resource Center:

<http://training.fema.gov/EMIWeb/IS/IS860a/CIRC/index.htm>.

**Critical Infrastructure Training Module** provides an overview of the National Infrastructure Protection Plan (NIPP) and critical infrastructure Annex to the National Response Framework. The module is available upon request in PowerPoint format with instructor and participant guides and can be easily integrated into existing training programs. A Spanish version is also available. To request the training module, contact [IP\\_Education@hq.dhs.gov](mailto:IP_Education@hq.dhs.gov).

**Critical Infrastructure Sector Snapshots** provide a quick look at SOPD sectors and generally contain sector overviews; information on sector partnerships; information on critical infrastructure protection issues and priority programs. For more information, see [http://www.dhs.gov/xlibrary/assets/nipp\\_annrpt.pdf](http://www.dhs.gov/xlibrary/assets/nipp_annrpt.pdf). For more information, contact [NIPP@dhs.gov](mailto:NIPP@dhs.gov).

**DHS Center of Excellence: Global Terrorism Database** is an open-source database including information on terrorist events around the world from 1970 through 2010 (with additional updates planned for the future). For more information, see [www.start.umd.edu/gtd](http://www.start.umd.edu/gtd).

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

**DHS Center of Excellence: National Consortium for the Study of Terrorism and Responses to Terrorism (START)** informs decisions on how to disrupt terrorists and terrorist groups, while strengthening the resilience of U.S. citizens to terrorist attacks. For more information, see [www.start.umd.edu](http://www.start.umd.edu).

**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/ExpertJudgmentElicitationMethods.pdf> or contact [universityprograms@dhs.gov](mailto:universityprograms@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](http://www.dhs.gov/niac).

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

**NPPD/IP SOPD Critical Infrastructure Sector Snapshots, Fact Sheets and Brochures** These two-page snapshots provide a quick look at each of the eighteen sectors and generally contain sector

overviews; information on sector partnerships; critical infrastructure protection challenges; and priority programs. For more information, see [http://www.dhs.gov/files/programs/gc\\_1189168948944.shtm](http://www.dhs.gov/files/programs/gc_1189168948944.shtm).”

**Protective Security Advisors (PSAs)** are DHS/NPPD/IP infrastructure security experts deployed across the country who serve as the link between state, local, tribal, territorial, and private sector organizations and DHS infrastructure protection resources. PSAs assist with ongoing state and local critical infrastructure and key resources security efforts, coordinate vulnerability assessments and training, support incident management, and serve as a vital channel of communication between private sector owners and operators of CIKR assets and DHS. Private sector owners and operators interested in contacting their PSA should contact [FOAnalysts@hq.dhs.gov](mailto:FOAnalysts@hq.dhs.gov) or (703) 235-9349.

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

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

## Critical Manufacturing

### Critical Manufacturing Cybersecurity Tabletop Exercise

In partnership with Critical Manufacturing SCC 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](mailto: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, see [www.dhs.gov/CIKR](http://www.dhs.gov/CIKR) or email [CriticalManufacturing@dhs.gov](mailto:CriticalManufacturing@dhs.gov).

**Critical Manufacturing Partnership Road Show** This program provides Critical Manufacturing Sector members an opportunity to participate in onsite visits

to various DHS locations. The visits include briefings on current threats to the U.S., including to the Critical Manufacturing Sector and related infrastructure. For more information, see [www.dhs.gov/CIKR](http://www.dhs.gov/CIKR) or email [CriticalManufacturing@dhs.gov](mailto:CriticalManufacturing@dhs.gov).

**SOPD/TSA Joint Exercise Program** This program allows Critical Manufacturers to develop advanced tabletop exercises that determine gaps and mitigate vulnerabilities in their respective transportation supply chains within the U.S. and cross border (particularly Canada and Mexico). This is a combined program with the Transportation Security Administration (TSA) with support from TSA's Intermodal Security Training and Exercise Program (ISTEP). For more information, please contact the NPPD/IP Critical Manufacturing SSA at [CriticalManufacturing@hq.dhs.gov](mailto: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/attrso/event/registration.html>. After submitting the short registration information to include setting a password of your choice, you will receive an email confirmation with instructions for logging in to view the material. Also includes One-pager/factsheet. For more information, please contact the Commercial Facilities SSA at [CFSTeam@dhs.gov](mailto:CFSTeam@dhs.gov).

**DHS Retail Video: "What's in Store - Ordinary People/Extraordinary Events"** The Department of Homeland Security's, Infrastructure Protection's Partnership and Outreach Division, Office for Bombing Prevention and the Commercial Facilities Sector-Specific Agency created a multimedia training video for retail employees of commercial shopping venues to alert them of the signs of suspicious behavior in the workplace. The video is intended to both highlight suspicious behavior, as well as encourage staff to take action when suspicious

behavior is identified. The video can be viewed at [http://www.dhs.gov/multimedia/dhs\\_retail\\_video\\_mv](http://www.dhs.gov/multimedia/dhs_retail_video_mv). For more information, please contact the NPPD/IP Commercial Facilities SSA at [CFSTeam@dhs.gov](mailto:CFSTeam@dhs.gov).

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

**Evacuation Planning Guide for Stadiums** This product was developed to assist stadium owners and operators with preparing an Evacuation Plan and determining when and how to evacuate, conduct shelter-in-place operations, or relocate stadium spectators and participants. For more information, contact [CFSTeam@hq.dhs.gov](mailto:CFSTeam@hq.dhs.gov).

**Hotel and Lodging Advisory Poster** This poster was created for all staff throughout the U.S. Lodging Industry to increase awareness regarding a property's potential to be used for illicit purposes, suspicious behavior and items, and appropriate actions for employees to take if they notice suspicious activity. The poster was designed in tandem with the Commercial Facilities SCC and the Lodging Subsector and is available at [http://www.dhs.gov/xlibrary/assets/ip\\_cikr\\_hotel\\_advisory.pdf](http://www.dhs.gov/xlibrary/assets/ip_cikr_hotel_advisory.pdf). For more information, please contact the NPPD/IP Commercial Facilities SSA at [CFSTeam@dhs.gov](mailto:CFSTeam@dhs.gov).

**Infrastructure Protection Sector-Specific Table Top Exercise Program (SSTEP) for the Commercial Facilities Retail/Lodging Subsectors and Sports Leagues/Public Assembly Subsectors** These tools are unclassified, adaptable and immediately deployable exercises which focus on information sharing which can be utilized by retail/lodging and outdoor

venues/sports leagues organizations at their facilities. In addition to the exercise scenario and slide presentation, users will find adaptable invitational communication tools, as well as the after action report template and participant surveys which will assist in incorporating change and developing improvement plans accordingly. The Retail/Lodging and Sports Leagues/Outdoor Venues SSTEPs will allow participants the opportunity to gain an understanding of issues faced prior to, during, and after a terrorist threat/attack and the coordination with other entities, both private and government, regarding a specific facility. For more information, please contact the NPPD/IP Commercial Facilities SSA at [CFSTeam@dhs.gov](mailto:CFSTeam@dhs.gov).

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

**IS-907 Active Shooter: What You Can Do** This online training provides guidance to individuals, including managers and employees, so that they can prepare to respond to an active shooter situation. The course is self-paced and takes about 45 minutes to complete. This comprehensive cross-sector training is appropriate for a broad audience regardless of knowledge and skill level. The training uses interactive scenarios and videos to illustrate how individuals who become involved in an active shooter situation should react. Topics within the course include: the actions one should take when confronted with an active shooter and responding law enforcement officials; how to recognize potential

indicators of workplace violence; the actions one should take to prevent and prepare for potential active shooter incidents; how to manage an active shooter incident. This course also features interactive knowledge reviews, a final exam, and additional resources. A certificate is given to participants who complete the entire course. The training may be accessed on the Federal Emergency Management Agency Emergency Management Institute Web site: <http://training.fema.gov/EMIWeb/IS/IS907.asp>. For more information about Office of Infrastructure Protection training courses, please contact: [IP\\_Education@hq.dhs.gov](mailto:IP_Education@hq.dhs.gov).

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

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

**Risk Self-Assessment Tool for Stadiums and Arenas, Performing Art Centers, Lodging, Convention Centers, Racetracks, and Parks and Fairgrounds** The Risk Self Assessment Tool (RSAT) is a secure, Web-based application designed to assist managers of stadiums and arenas with the identification and management of security vulnerabilities to reduce risk to their facilities. The RSAT application uses facility input in combination with threat and consequence estimates to conduct a comprehensive risk assessment and provides users with options for consideration to improve the security posture of their facility. It is also accompanied by a Fact Sheet/Brochure. For more information, please contact the NPPD/IP Commercial Facilities SSA at [CFSTeam@dhs.gov](mailto:CFSTeam@dhs.gov) or [RSAT@hq.dhs.gov](mailto:RSAT@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 HSIN-CS Commercial Facilities portal at <https://connect.hsin.gov/p21849699/>. For more information, contact the Commercial Facilities SSA at [CFSTeam@hq.dhs.gov](mailto:CFSTeam@hq.dhs.gov).

## Dams Security

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

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

**Consequence-Based Top Screen Fact Sheet** This fact sheet provides information pertaining to the Consequence-Based Top Screen (CTS) methodology, including how it was developed, its primary purpose, and the Web-based tool with which it is implemented. For more information, see [http://www.dhs.gov/files/programs/gc\\_1260541882284.shtm](http://www.dhs.gov/files/programs/gc_1260541882284.shtm) or contact the NPPD/IP Dams SSA at [Dams@dhs.gov](mailto:Dams@dhs.gov).

**Dams Sector Analysis Tool** is an integrated data management system and dams-specific analysis tool that establishes an integrated analysis gateway for all Dams Sector-related tools and information, which allows for a single source for data input and analysis. For more information, contact the Dams SSA at [dams@dhs.gov](mailto:dams@dhs.gov).

**Dams Sector Consequence-Based Top Screen (CTS) Tool** The purpose of the CTS methodology is to identify critical facilities within the Dams Sector (e.g., those high-consequence facilities, the failure or disruption of which could be potentially associated with the highest possible impact among sector assets). By focusing on potential consequences and decoupling the analysis from the threat and vulnerability components of the risk process, the CTS approach can serve as an effective all-hazards preliminary prioritization scheme. It is also accompanied by Fact Sheet/Brochure. For more information, please contact the NPPD/IP Dams SSA at [Dams@dhs.gov](mailto:Dams@dhs.gov).

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

**Dams Sector Crisis Management Handbook** Provides owners/operators with information relating to emergency response and preparedness issues; includes recommendations for developing emergency action plans and site recovery plans. The handbook is available at <http://www.damsafety.org/media/Documents/Security/DamsSectorCrisisManagementHandbook.pdf>. For more information, please contact the NPPD/IP Dams SSA at [Dams@dhs.gov](mailto:Dams@dhs.gov).

**Dams Sector Roadmap to Secure Control Systems** provides a comprehensive framework and recommended strategies focused on the protection of

industrial control systems across the Dams Sector in order to enhance the sector's understanding and management of cyber risks; facilitate the identification of practical risk mitigation solutions; promote information sharing; and improve sector-wide awareness of cyber security concerns. For more information, please contact the NPPD/IP Dams SSA at [Dams@dhs.gov](mailto:Dams@dhs.gov).

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

**Dams Sector Security Awareness Guide** This is a non-FOUO version of the Dam Sector Security Awareness Handbook for distribution to owners/operators. The guide is available at [http://www.damsafety.org/media/documents/DownloadableDocuments/DamsSectorSecurityAwarenessGuide\\_508.pdf](http://www.damsafety.org/media/documents/DownloadableDocuments/DamsSectorSecurityAwarenessGuide_508.pdf). For more information, please contact the NPPD/IP Dams SSA at [Dams@dhs.gov](mailto:Dams@dhs.gov).

**Dams Sector Tabletop Exercise Toolbox (DSTET)** – This tool was developed to assist sector stakeholders in planning and conducting a security-based tabletop exercise that is compliant with the Homeland Security Exercise and Evaluation Program. Multiple videos and examples are included as part of the tool for use during the exercise as “scene-setters.” The toolbox includes several modules, which can be tailored to accommodate specific needs at a given facility. The toolbox will assist owners and responders in

reviewing information sharing and coordination activities when dealing with a security incident and supports the identification of potential opportunities for improvement, thus enhancing overall incident response planning. The toolbox includes planner instructions, facilitator briefing slides and handbook, situation manual, sample invitation letters, sample feedback forms, and exercise reference materials. For more information, please contact the NPPD/IP Dams SSA at [Dams@dhs.gov](mailto:Dams@dhs.gov).

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

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

**IS-870 Dams Sector: Crisis Management Overview** is web-based training focused on information provided within the Dams Sector Crisis Management handbook. To access this course: <http://training.fema.gov/EMIWeb/IS/is870.asp>. For more information, please contact the NPPD/IP Dams SSA at [Dams@dhs.gov](mailto:Dams@dhs.gov).

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

**IS-872 Dams Sector: Protective Measures (FOUO)** This Web-based training focuses on information provided within the Dams Sector Protective Measures handbook. To access this course:

<http://training.fema.gov/EMIWeb/IS/is872.asp>. For more information, please contact the NPPD/IP Dams SSA at [Dams@dhs.gov](mailto:Dams@dhs.gov).

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

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

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

**Security Awareness for Levee Owners Brochure** This brochure provides succinct information on surveillance indicators and incident reporting. The brochure is available at <http://training.fema.gov/EMIWeb/IS/IS860a/CIKR/assets/SecurityAwarenessForLeveeOwnersBrochure.pdf>. For more information, please contact the NPPD/IP Dams SSA at [Dams@dhs.gov](mailto:Dams@dhs.gov).

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

**Suspicious Activity Reporting Fact Sheet** provides information regarding the online Suspicious Activity Reporting tool within the HSIN-CS Dams Portal that was established to provide sector stakeholders with the capability to report and retrieve information pertaining to suspicious activities that may potentially be associated with pre-incident surveillance, and those activities related to the exploration or targeting of a specific critical infrastructure facility or system. For more information, contact the Dams SSA at [dams@dhs.gov](mailto:dams@dhs.gov).

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

**Security Awareness for Levee Owners Brochure** provides information on surveillance indicators and incident reporting. For more information, see [https://www.dhs.gov/files/programs/gc\\_12838780\\_65033.shtm](https://www.dhs.gov/files/programs/gc_12838780_65033.shtm) or contact the Dams SSA at [dams@dhs.gov](mailto:dams@dhs.gov).

## Food Safety and Influenza

**DHS Center of Excellence: Center for Advancing Microbial Risk Assessment (CAMRA)**, co-led by Michigan State University and Drexel University and established jointly with the U.S. Environmental Protection Agency, fills critical gaps in risk assessments for decontaminating microbiological threats — such as plague and anthrax — answering the question, “How Clean is Safe?” Resources include: Water mixing and pathogen dilution models; dose response models for Category A bioterror agents; and the Knowledge Warehouse, an online repository of microbial risk assessment information highlighting

connections between projects. For more information, visit <http://camra.msu.edu> or email [camra@msu.edu](mailto:camra@msu.edu).

**DHS Center of Excellence: National Center for Zoonotic and Animal Disease Defense (ZADD)** conducts research to protect against the introduction of high-consequence foreign animal and zoonotic diseases into the United States, with an emphasis on prevention, surveillance, intervention and recovery. Resources include Emergency Response Support System; Animal Health Network; Courses on Foreign Animal and Zoonotic Diseases, Public and Private sector Awareness Materials, Field Guide to Handling Contaminated Animal and Plant Materials, Mass Livestock Carcass Management workshop, Specialists in Foreign Animal and Zoonotic Diseases, an Avian Influenza Study Curriculum, a Guide to Developing an Animal Issues Emergency Management Plan, The Biosecurity Research Institute (BRI) and a compilation of materials pertaining to the Economic Impact of Foreign Animal Diseases to the United States. For more information, see <http://fazd.tamu.edu/> or <http://www.ceedad.org> or contact [universityprograms@dhs.gov](mailto:universityprograms@dhs.gov).

**DHS Center of Excellence: National Center for Food Protection and Defense (NCFPD)** establishes best practices, develops new tools, and attracts new researchers to prevent, manage and respond to food contamination events. Resources include: Food and Agriculture Criticality Assessment Tool (FAS-CAT); FoodSHIELD, a web-based system for communication, coordination, community-building, education, and training among the Nation’s food and agriculture sectors; Global Chronology of Incidents of Chemical, Biological, Radioactive and Nuclear Attacks from 1961-2005; Mass Production of Detection and Neutralizing Antibodies; Food Protection and Food Safety and Defense Graduate Certificate Programs; Risk Communication, Message Development/Evaluation and Training; decontamination protocols; and Regulatory, Policy, Technical, and Practical Issues related to Contaminated Food Disposal. For more information, see <http://www.ncfpd.umn.edu/> or contact [universityprograms@dhs.gov](mailto:universityprograms@dhs.gov).

**DHS Pandemic Influenza Impact on Communications Network Study and Best Practices** evaluates the potential impact on the communications infrastructure in the event of a pandemic influenza in the U.S. The study examines potential communications and information technology issues during a pandemic and identifies industry and government recommendations on how to better prepare the nation to handle these challenges. The study is available at [http://www.ncs.gov/library/pubs/Pandemic%20Comms%20Impact%20Study%20\(December%202007\).pdf](http://www.ncs.gov/library/pubs/Pandemic%20Comms%20Impact%20Study%20(December%202007).pdf). For more information, contact [ncsweb1@dhs.gov](mailto:ncsweb1@dhs.gov).

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

**Sector-Specific Pandemic Influenza Guides** NPPD/IP developed sector-specific guides for pandemic influenza for the Chemical, Commercial Facilities, Dams, Emergency Services, and Nuclear Sectors. For more information, please contact the NPPD/IP Sector Outreach and Programs Division at [SOPDExecSec@dhs.gov](mailto:SOPDExecSec@dhs.gov).

## Hazardous Materials Transportation Security

**Federal Motor Carrier Safety Administration: Guide to Developing an Effective Security Plan for the Highway Transportation of Hazardous Materials** is a tool that motor carriers transporting hazardous materials can use in developing a security plan as required by the U.S. Department of Transportation in

their HM-232 rulemaking [1]. It is designed to provide motor carriers with (a) sufficient background to understand the nature of the threats against hazardous materials transportation; (b) the means to identify the vulnerabilities to those threats; and (c) an approach to address the vulnerabilities. For more information, see [http://www.tsa.gov/assets/pdf/guide\\_security\\_plan.pdf](http://www.tsa.gov/assets/pdf/guide_security_plan.pdf). Contact the TSA Highway and Motor Carrier offices at [highwaysecurity@dhs.gov](mailto:highwaysecurity@dhs.gov).

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

**Hazmat Motor Carrier Security Self-Assessment Training Program** addresses the requirements contained in 49 Code of Federal Regulations (CFR), Part 172.802, which requires motor carriers that transport placarded amounts of hazardous materials to develop a plan that adequately addresses security risks related to the transportation of hazardous materials. Training materials can be found at [http://www.tsa.gov/what\\_we\\_do/tsnm/highway/self\\_training.shtm](http://www.tsa.gov/what_we_do/tsnm/highway/self_training.shtm). Contact TSA Highway and Motor Carrier Division at [highwaysecurity@dhs.gov](mailto: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 particular circumstances. For more information, see [http://www.tsa.gov/what\\_we\\_do/tsnm/highway/hssm\\_sai.shtm](http://www.tsa.gov/what_we_do/tsnm/highway/hssm_sai.shtm) or contact [highwaysecurity@dhs.gov](mailto:highwaysecurity@dhs.gov).

**Pipeline and Hazardous Materials Safety Administration: Risk Management Self-Evaluation Framework (RMSEF)** provides a basic framework for

managing risk as part of the hazardous materials transportation process. RMSEF is a tool for all parties (regulators, shippers, carriers, emergency response personnel, etc.) to look at their operations and consider how they assess and manage risk. For more information, see <http://www.phmsa.dot.gov/hazmat/risk/rmsef> or contact [highwaysecurity@dhs.gov](mailto:highwaysecurity@dhs.gov)

## Land Transportation and Pipeline

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

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

**First Observer™ Training** TSA provides funding for the First Observer™ program under the Trucking Security Program grant. The First Observer™ website has online training modules for trucking, school buses, law enforcement, cargo, hazmat, highway workers, among others. You can log on to the website for training at: <http://www.firstobserver.com/training/home.php> or contact or [Firstobserver@hms-world.com](mailto:Firstobserver@hms-world.com) (888) 217-5902.

**Highway and Motor Carrier Awareness Posters** include Motorcoach Awareness Posters for terminals: "Watch for Suspicious Items" and "Watch for Suspicious Behaviors" for terminals as well as a School Transportation Employee Awareness poster. For more information, see [http://www.tsa.gov/what\\_we\\_do/tsnm/highway/documents\\_reports.shtm](http://www.tsa.gov/what_we_do/tsnm/highway/documents_reports.shtm) or contact [highwaysecurity@dhs.gov](mailto:highwaysecurity@dhs.gov).

**Highway ISAC** The TSA Trucking Security Program funds the First Observer™ domain awareness program as well as a Call-Center and Information Sharing and Analysis Center (ISAC). The Highway ISAC creates products and bulletins and e-mails them to a distribution list from TSA Highway and Motor Carrier and the First Observer program. For more information, contact [www.firstobserver.com](http://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](mailto:HSIN.helpdesk@dhs.gov) (866) 430-0162.

**Intermodal Security Training and Exercise Program (I-STEP)** supports TSA's Transportation Sector Network Management (TSNM) Modal Security Managers with exercises and training. The program is designed to support all transportation security partners with security objectives and training that has clear and consistent performance measures. For more

information, see [http://www.tsa.gov/what\\_we\\_do/layers/istep/index.shtm](http://www.tsa.gov/what_we_do/layers/istep/index.shtm) or contact [i-step@dhs.gov](mailto:i-step@dhs.gov) (571) 227-5150.

**Laminated Security Awareness Driver Tip Card** contains the following topics: bus operator alerts; hijacking; evacuating the vehicle; awareness and what to look for; and possible chemical/biological weapons. For more information, see [http://www.tsa.gov/what\\_we\\_do/tsnm/highway/documents\\_reports.shtm](http://www.tsa.gov/what_we_do/tsnm/highway/documents_reports.shtm) or contact [highwaysecurity@dhs.gov](mailto:highwaysecurity@dhs.gov).

**Land Transportation Antiterrorism Training Program (LTATP)** is an effort by the Federal Law Enforcement Training Center to enhance knowledge, skills, and capabilities of law enforcement and security officials to prevent acts of terrorism. Through a curriculum focused on surface transportation security, this five-day program provides the participants with tools to protect the land transportation infrastructure, including rail, mass transit and bus operations, and most importantly passengers and employees. For more information, see <http://www.fletc.gov/training/programs/counterterrorism-division/land-transportation-antiterrorism-training-program-ltatp> or contact: [FLETC-CounterterrorismDivision@hq.dhs.gov](mailto:FLETC-CounterterrorismDivision@hq.dhs.gov).

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

**Operation Secure Transport (OST)** is security awareness training for the over-the-road bus industry. The training program will be available on CD and online. The training modules will be broken down into the following categories: driver; maintenance; terminal employees; management; and crisis response. For more information, see [http://www.tsa.gov/what\\_we\\_do/tsnm/highway/motorcoach.shtm](http://www.tsa.gov/what_we_do/tsnm/highway/motorcoach.shtm) or contact [highwaysecurity@dhs.gov](mailto:highwaysecurity@dhs.gov).

**Pipeline Security Awareness for the Pipeline Industry Employee Training CD and Brochures** are a security awareness trainings centered on heightening pipeline employee awareness of suspicious activity and their importance in keeping our Nation's pipeline system secure. To further enhance the information contained in the pipeline security awareness training CD, TSA produced the brochures "Pipeline Security Awareness for Employees" and "Good Neighbors! A Pipeline Security Neighborhood Watch." The CD and brochures may be requested on the TSA Pipeline Security website at [http://www.tsa.gov/what\\_we\\_do/tsnm/pipelines/training.shtm](http://www.tsa.gov/what_we_do/tsnm/pipelines/training.shtm). For more information contact the Pipeline Security Division at [PipelineSecurity@dhs.gov](mailto:PipelineSecurity@dhs.gov).

**Pipeline Security Guidelines** In April 2011, TSA released Pipeline Security Guidelines that supersede previous federal documents as the primary guide for pipeline industry security. The GUIDELINES are intended to be used by natural gas and hazardous liquid transmission pipeline companies, natural gas distribution companies and liquefied natural gas facility operators. For more information, see [http://www.tsa.gov/what\\_we\\_do/tsnm/pipelines/resources.shtm](http://www.tsa.gov/what_we_do/tsnm/pipelines/resources.shtm) or contact [PipelineSecurity@dhs.gov](mailto:PipelineSecurity@dhs.gov).

**Protecting Pipeline Infrastructure: The Law Enforcement Role** is a DVD intended to enhance the law enforcement community's understanding of pipeline systems and their security issues. The DVD provides a basic understanding of how pipeline systems function, the principle products they transport, and includes a discussion of the threats and

vulnerabilities to pipelines. The primary audience for this DVD is local, state, and federal law enforcement, federal security partners, and others involved with infrastructure security. Viewers should come away with a better understanding of the typical measures taken to protect pipelines and actions they can take to assist pipeline operators during times of heightened security alert. For more information and to request a copy see

[http://www.tsa.gov/what\\_we\\_do/tsnm/pipelines/training.shtm](http://www.tsa.gov/what_we_do/tsnm/pipelines/training.shtm)

**Safeguarding America's Transportation System Security Guides** are available for highway passenger security motorcoach personnel, private and contract carrier company employees, Owner-Operator Independent Drivers Association (OODA) 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](http://www.tsa.gov/highway). For more information, contact [highwaysecurity@dhs.gov](mailto:highwaysecurity@dhs.gov).

**School Transportation Security Awareness (STSA)** training provides school bus drivers, school administrators, and staff members with information that will enable them to effectively identify and report perceived security threats, as well as the skills to appropriately react and respond to a security incident should it occur. For more information, see [http://www.tsa.gov/what\\_we\\_do/tsnm/highway/stsa.shtm](http://www.tsa.gov/what_we_do/tsnm/highway/stsa.shtm), or contact [highwaysecurity@dhs.gov](mailto:highwaysecurity@dhs.gov).

**Transit Agency Security and Emergency Management Protective Measures** is a compilation of recommended protective measures for threat levels under the National Terrorism Alert System. This product has been developed as a technical resource to transit agency executive management and senior staff assigned to develop security and emergency response plans and to implement protective measures for response to the NTAS threat conditions and emergencies that might affect a transit agency. For more information, see

[http://www.tsa.gov/assets/pdf/mass\\_transit\\_protective\\_measures.pdf](http://www.tsa.gov/assets/pdf/mass_transit_protective_measures.pdf) or contact [MassTransitSecurity@dhs.gov](mailto:MassTransitSecurity@dhs.gov).

### **Transportation Security Grant Program (TSGP)**

provides security grants to transit systems, intercity bus companies, freight railroad carriers, ferries, and the trucking industry to help protect the public and the nation's critical transportation infrastructure. The grants support high-impact security projects that have a high efficacy in reducing the most risk to our nation's transportation systems. For more information, see <http://www.fema.gov/government/grant/tsgp/> or contact [askcsid@dhs.gov](mailto:askcsid@dhs.gov), 800-368-6498.

### **Transportation Sector Network Management Highway and Motor Carrier Division Annual Report**

TSA Highway and Motor Carrier Division publishes an Annual Report and posts the document on the following website [http://www.tsa.gov/what\\_we\\_do/tsnm/highway/documents\\_reports.shtm](http://www.tsa.gov/what_we_do/tsnm/highway/documents_reports.shtm).

**TSA Counterterrorism Guides** are designed for highway transportation security partners in the trucking, highway infrastructure, motorcoach, and school transportation industries. These guides are small flip-charts containing the following topics: pre-incident indicators; targets; threats to highway; insider threat; cloned vehicle; hijacking prevention; suspicious packages; information on explosive devices; prevention/mitigation; security planning; security inspection checklist; security exercises; chemical/biological/nuclear/radiological incidents; and federal, state and local POCs. You can contact TSA HMC to order a copy, pending available inventory at [highwaysecurity@dhs.gov](mailto: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://www.aww-sp.com/Americas\\_Waterway\\_Watch/Home.html](http://www.aww-sp.com/Americas_Waterway_Watch/Home.html) or contact [aww@uscg.mil](mailto: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 HSCs also have their own state or locally-sponsored websites, maintained separately from USCG Homeport. All U.S. critical ports have Area Committees and Area Contingency Plans. See the AMSC, Area Committee and HSC postings at [www.homeport.uscg.mil](http://www.homeport.uscg.mil).

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

**The Coast Guard Journal of Safety at Sea** is the voice of the Coast Guard Marine Safety and Security Council and is published quarterly with over 30,000 copies mailed out for each issue. The audience includes a large segment of the private maritime industry population, including retired officers, fishing vessel captains, river pilots, ocean scientists, marine engineers, tug/tow boat operators, shipping executives, insurance operators, and maritime lawyers. Issues of Proceedings are available to the public at [www.uscg.mil/proceedings](http://www.uscg.mil/proceedings).

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

**DHS Center of Excellence: Center for Maritime, Island, & Remote/Extreme Environment Security (MIREES)** is led by the University of Hawaii in Honolulu for maritime and island security and Stevens Institute of Technology in Hoboken, N.J., for port security. The MIREES strengthens maritime domain awareness and safeguards populations and properties unique to U.S. islands, ports, and remote and extreme environments. For more information, see <http://cimes.hawaii.edu/> and <http://www.stevens.edu/csr/> or contact [universityprograms@dhs.gov](mailto:universityprograms@dhs.gov).

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

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

**Maritime Passenger Security Courses** address topics to improve passenger vessel employee security awareness in their operating environments and to increase the effectiveness of their responses to suspicious items and persons that they might encounter. Courses available include: "Security Awareness For Passenger Vessel Employees," "IED/VBIED Recognition and Response for Passenger Vessels and Terminals," and "Crowd Control for Passenger Vessels and Terminals," and "Maritime Terrorism and Hijacking Situations." To order, contact TSA Port & Intermodal Security Division at [Maritime@dhs.gov](mailto:Maritime@dhs.gov) (571) 227-3556.

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

**Port Interagency Information Sharing Assessment** consists of a recurring process of interviews with

Coast Guard Sector personnel and selected federal, state, local personnel, and private partners who participate in joint maritime planning, prevention, response and recovery missions. Port Interagency Information Sharing reports are currently only released to the participants, although a publicly-releasable version of the report is under consideration for 2012. To schedule participation in next year's annual interviews, please contact the study team at [uscginformationsharing@uscg.mil](mailto:uscginformationsharing@uscg.mil).

**Port Security Grant Program** is a sustainable, risk-based effort to protect critical port infrastructure from terrorism, particularly attacks using explosives and non-conventional threats that could cause major disruption to commerce. The PSGP provides grant funding to port areas for the protection of critical port infrastructure from terrorism. For more information, visit <http://www.fema.gov/government/grant/> or contact [askcsid@dhs.gov](mailto:askcsid@dhs.gov) (800) 368-6498.

**Secure Freight Initiative (SFI) and Importer Security Filing and additional carrier requirements (10+2)** The Secure Freight Initiative, through partnerships with foreign governments, terminal operators, and carriers, enhances the DHS capability to assess the security of U.S.-bound maritime containers by scanning them for nuclear and other radioactive materials before they are laden on vessels bound for the U.S. For more information, please visit [http://www.cbp.gov/xp/cgov/trade/cargo\\_security/carriers/security\\_filing/](http://www.cbp.gov/xp/cgov/trade/cargo_security/carriers/security_filing/) or contact [securefreightinitiative@dhs.gov](mailto:securefreightinitiative@dhs.gov).

**Transportation Worker Identification Credential (TWIC)** is a security program designed to ensure that individuals who pose a security threat do not gain unescorted access to secure areas of the Nation's maritime transportation system. The credential is a biometric card that ensures only vetted workers can enter without an escort to secure transportation areas. The TWIC Program is jointly administered by TSA and the U.S. Coast Guard. For more information, see [http://www.tsa.gov/what\\_we\\_do/layers/twic/index.shtm](http://www.tsa.gov/what_we_do/layers/twic/index.shtm), or contact (866) 347-8942.

**U.S. Coast Guard Auxiliary** is the uniformed volunteer component of the United States Coast Guard. The Auxiliary conducts safety patrols on local waterways, assists the Coast Guard with homeland security duties, teaches boating safety classes, conducts free vessel safety checks for the public, and performs many other support activities. The Auxiliary has members in all 50 states, Puerto Rico, the Virgin Islands, American Samoa and Guam. For more information, visit <http://www.cgaux.org/>.

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

**U.S. Coast Guard Navigation Center** supports safe and efficient maritime transportation by delivering accurate and timely maritime information, vessel monitoring system support and Global Position System (GPS) augmentation signals that permit high-precision positioning and navigation. For additional information, see <http://www.navcen.uscg.gov/>.

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

## Mass Transit and Rail Security

**Freight Rail Security Grant Program** funds freight railroad carriers, owners, and officers of railroad cars

to protect critical surface transportation infrastructure from acts of terrorism, major disasters and other emergencies. For more information, visit <http://www.fema.gov/government/grant/> or contact [askcsid@dhs.gov](mailto:askcsid@dhs.gov) (800) 368-6498.

**Homeland Security Information Network (HSIN) – Freight Rail Portal** has been designed to provide consistent, real time information sharing capabilities in an integrated, secure, web-based forum to coordinate and collaborate directly with our security partners. Membership to the Freight Rail portal is provided once vetted by portal administrators. For more information, contact [HSIN.helpdesk@dhs.gov](mailto:HSIN.helpdesk@dhs.gov) or [Linda.Lentini@dhs.gov](mailto:Linda.Lentini@dhs.gov) (866) 430-0162.

**Homeland Security Information Network – Public Transit Portal (HSIN-PT)** has been integrated into the HSIN network to provide one stop security information sources and outlets for security advisories, alerts and notices. Membership to the Public Transit portal is provided once vetted by portal administrators. For more information, contact [MassTransitSecurity@dhs.gov](mailto:MassTransitSecurity@dhs.gov).

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

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

**Keep the Nation’s Railroad Secure Brochure** assists railroad employees to recognize signs of a potential terrorist act. It is to be used in conjunction with a railroad company’s existing security policies and procedures and may be modified to display the company’s emergency contact information for ease of reference. See

[http://www.tsa.gov/what\\_we\\_do/tsnm/freight\\_rail/training.shtm](http://www.tsa.gov/what_we_do/tsnm/freight_rail/training.shtm) or contact [freightrailsecurity@dhs.gov](mailto: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](mailto:MassTransitSecurity@dhs.gov).

**Mass Transit and Passenger Rail – Field Operational Risk and Criticality Evaluation (FORCE)** is a threat-based, risk-managed protocol that evaluates threat, vulnerability, and consequence from a variety of vantage points, focusing primarily on the rail and bus properties but also surveying intermodal and interdependent critical infrastructure and key resources. It is also adaptable to assist with new start-up properties about to come online or transit agencies with aggressive future expansion initiatives as well as regions hosting special security events. For more information, contact [MassTransitSecurity@dhs.gov](mailto:MassTransitSecurity@dhs.gov).

**Mass Transit Employee Vigilance Campaign** The “NOT ON MY SHIFT” program employs professionally-designed posters to emphasize the essential role that mass transit and passenger rail employees play in security and terrorism prevention in their systems. Adaptable templates enable each transit agency to tailor the product to its operations by including the system logo, photographs of their own agency’s employees at work, and quotes from the senior leadership, law enforcement and security officials, or frontline employees. The personalized approach has proven effective in gaining employees’ attention and interest, supporting the participating

transit and rail agencies’ efforts to maintain vigilance for indicators of potential terrorist activity. TSA designs the posters based on the preferences of the particular mass transit or passenger rail agency. For more information contact [MassTransitSecurity@dhs.gov](mailto: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](mailto: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, see [http://www.tsa.gov/assets/pdf/TSGP\\_Training\\_IB24\\_3.pdf](http://www.tsa.gov/assets/pdf/TSGP_Training_IB24_3.pdf), for TSGP – Approved Training Programs, see [http://www.tsa.gov/assets/pdf/approved\\_vendor\\_list.pdf](http://www.tsa.gov/assets/pdf/approved_vendor_list.pdf) or [MassTransitSecurity@dhs.gov](mailto:MassTransitSecurity@dhs.gov).

**Mass Transit Smart Security Practices** is a compilation of smart security practices drawn from the results of the comprehensive security assessments completed under the Baseline Assessment for Security Enhancement (BASE) program. This compilation fosters communication nationally among security professionals in mass transit and passenger rail to expand adoption of effective practices, tailored as necessary to each agency operating environment. For

more information, contact [MassTransitSecurity@dhs.gov](mailto:MassTransitSecurity@dhs.gov).

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

**Rail Security Rule Overview** On November 26, 2008, DHS published a regulation governing security in the freight rail industry. The regulation not only affects freight railroads, but their customers as well. This presentation provides a high-level overview of the Rail Security Rule and information regarding the requirements of the regulation. For more information, see [http://www.tsa.gov/assets/pdf/rail\\_rule\\_overview\\_f\\_or\\_stakeholder\\_workshops\\_mar\\_09.pdf](http://www.tsa.gov/assets/pdf/rail_rule_overview_f_or_stakeholder_workshops_mar_09.pdf) or contact [Scott.Gorton@dhs.gov](mailto:Scott.Gorton@dhs.gov).

## Nuclear Security

**The Domestic Nuclear Detection Office (DNDO)** is a jointly staffed agency within the Department of Homeland Security. DNDO is the primary entity in the U.S. government for implementing domestic nuclear detection efforts for a managed and coordinated response to radiological and nuclear threats, as well as integration of federal nuclear forensics programs. Additionally, DNDO is charged with coordinating the development of the global nuclear detection and reporting architecture, with partners from federal, state, local, and international governments and the private sector. DNDO will also develop, acquire, and support the domestic nuclear detection and reporting system. DNDO's Commercial First Initiative will facilitate this by shifting the focus from government development of materiel solutions to a commercial first approach that will leverage

industry innovation and facilitate the deployment of detection equipment to DHS components and the state/local first responders. For more information, see [www.dhs.gov/xabout/structure/editorial\\_0766.shtm](http://www.dhs.gov/xabout/structure/editorial_0766.shtm) or contact [dndo.info@dhs.gov](mailto:dndo.info@dhs.gov).

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

**The Joint Analysis Center (JAC) Program** provides an Interagency coordination mechanism and central monitoring point for the Global Nuclear Detection Architecture (GNDA), maintains situational awareness across the GNDA – to include status of radiological and nuclear (rad/nuc) detection assets, visibility into the status of rad/nuc alarms, awareness of rad/nuc-related incidents and events, data, and trend analyses supporting GNDA operations. The JACCIS, an Information Technology (IT) system specifically developed to support JAC operations, is a secure web application and database which supports alarm adjudication, analysis, information sharing, and reporting for the Global Nuclear Detection Architecture (GNDA) by DNDO and its mission partners. Via its integral Nuclear Assessment Program (NAP), the JAC Program provides technical expertise toward specific requirements of DNDO to include the development of classified annexes for architectural studies; creation of GNDA visualization tools; operations support activities and the ongoing development and execution of red teaming and assessment activities. Specifically, NAP provides technical advice and assistance to DNDO operations and the supporting elements of the GNDA. For more information, see

[http://www.dhs.gov/xabout/structure/editorial\\_0766.shtm](http://www.dhs.gov/xabout/structure/editorial_0766.shtm).

**Monthly Unclassified Threat Briefing** The NPPD/IP Nuclear SSA holds an unclassified security teleconference for nuclear facility owners and operators, plant managers, and security professionals on the first Wednesday of every month. The teleconference covers significant changes to the threat environment, results of recent terrorism investigations, and other reported suspicious incidents. For more information, please contact the NPPD/IP Nuclear SSA at [NuclearSSA@hq.dhs.gov](mailto:NuclearSSA@hq.dhs.gov).

**National Nuclear Forensics Expertise Development Program (NNFEDP)** aims to provide a stable foundation from which to develop and sustain the nuclear forensics workforce. This interagency program is dedicated to maintaining a vibrant academic pathway from undergraduate to post-doctorate study in disciplines directly relevant to nuclear forensics, such as radiochemistry, geochemistry, nuclear physics, nuclear engineering, materials science, and analytical chemistry. The NNFEDP promotes a unique interdisciplinary approach that encourages collaboration among academic programs, universities, and the DOE national laboratories. Initiatives include undergraduate outreach and scholarships; graduate fellowships, internships, and mentoring; post-doctorate fellowships; university education awards; and junior faculty awards. For more information, see <http://scuref.org>, [http://www.dhs.gov/xabout/careers/gc\\_128680578\\_0388.shtm#2](http://www.dhs.gov/xabout/careers/gc_128680578_0388.shtm#2) or contact [dndo.info@dhs.gov](mailto:dndo.info@dhs.gov).

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

**Nuclear Sector Information Sharing Standard Operating Procedure (SOP)** This document is designed to enhance the effectiveness of voluntary information coordination and distribution among members of the Nuclear Sector Information Sharing Environment (ISE). For more information, please contact the NPPD/IP Nuclear SSA at [NuclearSSA@hq.dhs.gov](mailto: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](mailto:NuclearSSA@hq.dhs.gov).

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

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

**Open Access to ANSI N42 Series Standards** DNDO sponsors IEEE to provide copies of the ANSI N42 radiation detection standards free of charge to anyone who wants a copy. The web site to obtain the latest published version of one of the sponsored standards is: <http://standards.ieee.org/about/get/>

**Radiological Emergency Preparedness Program (REP)** helps to secure the health and safety of citizens living around commercial nuclear power plants. REP is responsible for review and final approval of all neighborhood radiological emergency plans. The REP program is a leader in areas of policy guidance, planning, training, public education and preparedness for nuclear power plants. For more information, visit

[http://www.fema.gov/about/divisions/thd\\_repp.shtm](http://www.fema.gov/about/divisions/thd_repp.shtm).

**Training, Exercise, and Assistance (TE&A) Program** The Global Nuclear Detection Architecture (GNDA) TE&A Program utilizes various types of engagements, collaborative dialogues, meetings, and exercises to develop and mature effective standards and protocols for radiological and nuclear detection (RND) capabilities to optimize GNDA nodes and their interactions among federal, state, local, and tribal jurisdictions. This includes the state and Local Working Group and Executive Steering Committee meetings, as part of a comprehensive effort to integrate and hone contributions with stakeholders to most effectively and efficiently perform their GNDA roles. It addresses interior and maritime RND programs and the Mobile Detection Deployment Project (MDDP), mobile equipment packages positioned strategically to support rad/nuc detection activities during periods of high demand. TE&A also develops and promotes radiological and nuclear detection training for federal, state and local law enforcement and public safety professionals to increase RND operational capabilities. Finally, it develops Homeland Security Exercise Evaluation Program (HSEEP) compliant, rad/nuc detection operational exercise templates for federal, state and local programs. This standards-based approach serves as an RND exercise force multiplier to improve overall domestic exercise efficiency and consistency across the GNDA. For more information, see [http://www.dhs.gov/xabout/structure/editorial\\_076\\_6.shtm](http://www.dhs.gov/xabout/structure/editorial_076_6.shtm).

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

## Physical Security Assessment Tools

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

**Comprehensive Security Assessments and Action Items** encompass activities and measures that are critical to an effective security program. The 17 Action Items cover a range of areas including security program management and accountability, security and emergency response training, drills and exercises, public awareness, protective measures for the National Terrorism Alert System threat levels, physical security, personnel security, and information sharing and security. The TSA Transportation Security Inspectors-Surface conduct security assessments under the Baseline Assessment for Security Enhancement (BASE) program that evaluate the posture of mass transit and passenger rail agencies in the Action Items in a comprehensive and systematic approach to elevate baseline security posture and enhance security program management and implementation. The results of the security assessments inform development of risk mitigation programs and resource allocations, most notably security grants. For more information, see

[http://www.tsa.gov/assets/pdf/mass\\_transit\\_action\\_items.pdf](http://www.tsa.gov/assets/pdf/mass_transit_action_items.pdf) or contact [MassTransitSecurity@dhs.gov](mailto:MassTransitSecurity@dhs.gov).

**Design-Basis Threat (DBT): An Interagency Security Committee Report (FOUO)** is a stand-alone threat analysis to be used with the *Physical Security Criteria for Federal Facilities: An ISC Standard*. The DBT document establishes a profile of the type, composition, and capabilities of adversaries. For more information, see [http://www.dhs.gov/files/committees/gc\\_1194978\\_268031.shtm](http://www.dhs.gov/files/committees/gc_1194978_268031.shtm) or contact [isc@dhs.gov](mailto:isc@dhs.gov).

**Enhanced Critical Infrastructure Protection (ECIP) Visits** are conducted by Protective Security Advisors (PSAs) in collaboration with critical infrastructure owners and operators to assess overall facility security and increase security awareness. ECIP Visits are augmented by the Infrastructure Survey Tool (IST), a web based tool that provides the ability to collect, process, and analyze ECIP survey data in real time. Data collected during an ECIP visit is consolidated in the IST and then weighted and valued, which enables DHS to develop ECIP metrics; conduct sector-by-sector and cross-sector vulnerability comparisons; identify security gaps and trends across critical infrastructure sectors and sub-sectors; and establish sector baseline security survey scores. Private sector owners and operators interested in an ECIP Visit should contact [FOBanalysts@hq.dhs.gov](mailto:FOBanalysts@hq.dhs.gov) or (703) 235-9349.

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

**Regional Resiliency Assessment Program (RRAP)** is a cooperative, DHS-led assessment of specific critical infrastructure and regional analysis of the surrounding infrastructure, including key interdependencies. Private sector owners and operators interested in receiving more information on the RRAP should

contact [IPassessments@hq.dhs.gov](mailto:IPassessments@hq.dhs.gov).

**Site Assistance Visits (SAVs)** Site Assistance Visits are non-regulatory risk-informed vulnerability assessments that assist critical infrastructure owners and operators in identifying vulnerabilities, protective measures, planning needs, and options for consideration to increase protection from, and resilience to, a wide range of hazards. Following the assessment, DHS provides owners and operators with a SAV report, protected as PCII. SAVs enhance critical infrastructure owners' and operators' overall capabilities and resources for identifying and mitigating vulnerabilities, detecting and preventing terrorist attacks, and responding to and recovering from all-hazards events. Private sector critical infrastructure owners and operators interested in receiving more information on SAVs should contact [IPassessments@hq.dhs.gov](mailto:IPassessments@hq.dhs.gov).

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

## Protecting, Analyzing, & Sharing Information

**Automated Critical Asset Management System (ACAMS)** is a secure, web-based portal developed in partnership with state and local communities and the State, Local, Tribal, Territorial Government Coordinating Council (SLTTGCC). ACAMS is designed to help state and local governments build critical infrastructure protection programs in their local

jurisdictions and implement the National Infrastructure Protection Plan (NIPP). ACAMS provides a set of tools and resources that help law enforcement, public safety, and emergency response personnel collect, prioritize, analyze, and visualize critical infrastructure to prepare, prevent, respond, and recover from an attack, natural disaster, or emergency. ACAMS is provided at no cost for state and local use and is protected from public disclosure through the Protected Critical Infrastructure Information (PCII) program. For more information, see [www.dhs.gov/ACAMS](http://www.dhs.gov/ACAMS) or contact [ACAMShelp@hq.dhs.gov](mailto: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](mailto:soc@us-cert.gov); (888) 282-0870.

**Daily Open Source Infrastructure Report** is collected each weekday as a summary of open-source published information concerning significant critical infrastructure issues. Each Daily Report is divided by the critical infrastructure sectors and key assets defined in the National Infrastructure Protection Plan. The DHS Daily Open Source Infrastructure Report is available on [DHS.gov](http://DHS.gov) and Homeland Security Information Network-Critical Sectors (HSIN-CS). For more information, see [http://www.dhs.gov/files/programs/editorial\\_0542.shtm](http://www.dhs.gov/files/programs/editorial_0542.shtm) or contact [CIKR.ISE@dhs.gov](mailto:CIKR.ISE@dhs.gov) (202) 312-3421.

**DHS Center of Excellence: National Center for Visualization and Data Analytics (CVADA)** creates the scientific basis and enduring technologies needed to analyze massive amounts of information from

multiple sources to more reliably detect threats to the security of the Nation, its infrastructures and to the health and welfare of its populace. These new technologies will also improve the dissemination of both information and related technologies. Co-led by Purdue University and Rutgers University, available educational opportunities are geared towards educating the next generation of homeland security professionals with initiatives that span the entire career development pipeline, ranging from K-12 programs through undergraduate and graduate level work, to professional education and training. For more information, see <http://www.purdue.edu/discoverypark/vaccine/> and <http://www.ccicada.org/> or contact [universityprograms@dhs.gov](mailto:universityprograms@dhs.gov).

**DHS Geospatial Information Infrastructure (GII)** is a body of geospatial data and application services built to meet common requirements across the DHS mission space. OneView (<https://gii.dhs.gov/oneview>) is a lightweight, web-based geographic visualization and analysis that provides a method for individual users to access and interact with all GII services. The GII also maintains the DHS Earth KML service, which provides authoritative infrastructure data and various static and dynamic situational awareness feeds in standard geographic information system (GIS) data formats to authorized Homeland Security Information Network (HSIN) users at the federal, state, and local levels and within the private sector. For more information, contact [iCAV.info@hq.dhs.gov](mailto:iCAV.info@hq.dhs.gov).

**DHS Open Source Enterprise Daily and Weekly Intelligence Reports** provide open source information on several topics of interest. The following are currently available open source reports: The DHS Daily Digest Report, The DHS Daily Cyber Report, The DHS Daily Human Trafficking and Smuggling Report, The DHS Daily Terrorism Report, and The DHS Weekly Weapons and Munitions Trafficking and Smuggling Report. These reports may be accessed on the Homeland Security Information Network (HSIN) or private sector partners may

request that they be added to distribution by e-mailing [OSINTBranchMailbox@hq.dhs.gov](mailto:OSINTBranchMailbox@hq.dhs.gov) with subject line reading "Request DHS Daily [name] Report".

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

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

**Homeland Security Information Network-Critical Sectors (HSIN-CS)** HSIN-CS is the primary information-sharing platform between the critical infrastructure sector stakeholders. With a library of products that increases on an average of every 2 hours, HSIN-CS enables federal, state, local and private sector critical infrastructure owners and operators to communicate, coordinate, and share sensitive and sector-relevant information to protect their critical assets, systems, functions and networks, at no charge to sector stakeholders. To request access to HSIN-CS, please contact [CIKRISEAccess@hq.dhs.gov](mailto:CIKRISEAccess@hq.dhs.gov). When

requesting access, please indicate the critical infrastructure sector to which your company belongs and include your name, company, official email address, and supervisor's name and phone number.

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

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

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

**Infrastructure Data Taxonomy (IDT)** Critical infrastructure and their elements can be described and categorized in various ways, which can result in inconsistent communication and hinder timely decision-making within the homeland security community. To prevent such problems, DHS uses an Infrastructure Data Taxonomy to enable transparent and consistent communication about Critical infrastructure between government and private sector partners with its structured terminology. The Infrastructure Data Taxonomy allows its users to designate an asset as belonging to a particular group, and then apply additional, associated taxonomy levels to detail the specifics of the asset and describe its functions. For more information, see [http://www.dhs.gov/files/publications/gc\\_1226595\\_934574.shtm](http://www.dhs.gov/files/publications/gc_1226595_934574.shtm) or visit <https://taxonomy.iac.anl.gov/> to use this tool or contact: [IDT@dhs.gov](mailto:IDT@dhs.gov).

**Infrastructure Information Collection System (IICS)** is a secure, web-based application designed to provide authorized users with the ability to easily access, search, retrieve, visualize, analyze, and export infrastructure data originating from multiple disparate sources through a single interface. The IICS enables access to infrastructure-related data that is owned and managed by IP through the Infrastructure Data Warehouse as well as infrastructure-related data from various other federal, state, and local infrastructure protection mission partners. For more information, contact [IICD-IICS@hq.dhs.gov](mailto:IICD-IICS@hq.dhs.gov).

**INFOGRAMS** The Emergency Management & Response-Information Sharing & Analysis Center (EMR-ISAC) was established to provide information services that support the infrastructure protection and resilience activities of all Emergency Services Sector (ESS) departments, agencies, and organizations (public and private) nation-wide. InfoGrams contain four short articles issued weekly about Critical Infrastructure Protection (CIP) and Critical Infrastructure Resiliency (CIR) trends and developments. To acquire a no-cost subscription to EMR-ISAC information, send an e-mail request to

[emr-isac@dhs.gov](mailto:emr-isac@dhs.gov); to inquire about the practice of CIP or CIR within an ESS organization, call 301-447-1325.

**Intelligence and Analysis Private Sector Partnership Program** provides private sector businesses, groups, and trade associations with tailored threat briefings to meet their security information needs. Additionally, the office creates intelligence products that are posted on the Homeland Security Information Network-Critical Sectors (HSIN-CS) portal for use by pre-cleared critical infrastructure owners and operators. For more information, see [www.dhs.gov/hsin](http://www.dhs.gov/hsin). To request access to HSIN-CS, e-mail [HSINCS@dhs.gov](mailto:HSINCS@dhs.gov). When requesting access, please indicate the critical infrastructure sector to which your company belongs and include your name, company, official e-mail address, and supervisor's name and phone number. For more information, contact [I&APrivateSectorCoordinator@hq.dhs.gov](mailto:I&APrivateSectorCoordinator@hq.dhs.gov) or call (202) 282-9881.

**Joint DHS/FBI Classified Threat and Analysis Presentations** provide classified intelligence and analysis presentations to mass transit and passenger rail security directors and law enforcement chiefs in more than 20 metropolitan areas simultaneously through the Joint Terrorism Task Force network secure video teleconferencing system. The briefings occur on an approximately quarterly to semi-annual basis, with additional sessions as threat developments may warrant. For more information, contact [MassTransitSecurity@dhs.gov](mailto:MassTransitSecurity@dhs.gov).

**National Information Exchange Model (NIEM) Program** is a federal, state, local and tribal interagency initiative providing a national approach and common vocabulary for information exchange. NIEM has a robust training curriculum that is accessible both in classroom and on-line. The primary audience for the NIEM Training Program is executives, project and program managers, architects and technical implementers within federal, state, local, tribal and private entities. Additional information on the

training courses and NIEM can be obtained by visiting [www.NIEM.gov](http://www.NIEM.gov) or e-mailing [NIEMPMO@NIEM.gov](mailto:NIEMPMO@NIEM.gov).

**National Science and Technology Council (NSTC) Subcommittee on Biometrics and Identity Management (BiDM)** encourages greater collaboration and sharing of information on biometric activities among government departments and agencies; commercial entities; state, regional, and international organizations; and the general public. For more information, see <http://www.biometrics.gov/nstc/Default.aspx> or contact [info@biometrics.org](mailto:info@biometrics.org).

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

**Protected Critical Infrastructure Information (PCII) Program** is an information sharing resource designed to facilitate the flow and exchange of critical infrastructure information (CII) between the private sector, DHS and federal, state, tribal and local government entities. Private sector entities can voluntarily submit their CII to the PCII Program for use in federal, state and local critical infrastructure protection efforts. Information about the PCII Program, including the CII Act of 2002, the Final Rule and the implementing regulation as well as the PCII Program Procedures Manual can be found at [www.dhs.gov/pcii](http://www.dhs.gov/pcii). For additional information, contact [pcii-info@dhs.gov](mailto:pcii-info@dhs.gov) or (202) 360-3023.

**SOPD Classified Threat Briefings** SOPD coordinates both regularly scheduled and incident-specific classified briefings for cleared sector partners. For more information, contact Sector Outreach & Programs Division at [SOPDExecSec@dhs.gov](mailto:SOPDExecSec@dhs.gov).

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

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

<https://www.tripwire.dhs.gov/IED/appmanager/IEDPortal/IEDDesktop?nfpb=true&pageLabel=LOGIN>.

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

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

**Unified Incident Command and Decision Support (UICDS)** is a national "middleware foundation" designed to support information sharing for the National Response Framework and the National Incident Management System, including the Incident Command System. UICDS middleware is transparent to system operators during operations and requires no special training. UICDS is owned by the federal government and available at no-cost. It is built around data standards and the National Information Exchange Model. UICDS enables information sharing across domains, roles, hazards, echelons and applications. UICDS allows information sharing between disparate,

proprietary emergency management applications. UICDS users share what, when and with whom they want in accordance with existing or emerging sharing agreements. Users of UICDS are emergency managers and incident commanders in Federal, state, local and tribal organizations as well as critical infrastructure owners/operators. Operational and demonstration pilot programs have been on-going in multiple locations throughout the United States. For more information about UICDS and to download the free software development kit, go to: [www.uicds.us](http://www.uicds.us).

**U.S. Coast Guard Maritime Information eXchange ("CGMIX")** makes U.S. Coast Guard (USCG) maritime information available on the public internet in the form of searchable databases. Much of the information on the CGMIX website comes from the USCG Marine Information for Safety and Law Enforcement (MISLE) information system. For more information, see <http://cgmix.uscg.mil/>.

**Virtual USA (vUSA)** integrates technologies, methodologies, and capabilities for sharing and collaborating using public, multi-jurisdictional, and private sector information for the purpose of protecting lives, property, and the environment. vUSA is improving emergency response by ensuring that practitioners at all levels have immediate access to the information they need to make decisions, when they need it. More information can be found at [www.firstresponder.gov](http://www.firstresponder.gov).

# Securing and Managing Our Borders

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

## Border Security

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

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

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

<http://uids.utep.edu/> or contact [universityprograms@dhs.gov](mailto:universityprograms@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://apps.cbp.gov/eallegations/>, or contact the Commercial Targeting and 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](http://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 (DHS). 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 also has the ability to 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](http://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 <http://www.ice.gov/best/>.

**Project Shield America (PSA)** is the first line of defense against those who compromise U.S. national security by violating export laws, sanctions and

embargoes. Specifically, the ICE Counter-Proliferation Investigations Unit reaches out to applicable high-tech industries to monitor weapons of mass destruction and their components that are potential targets for illegal trafficking. Through PSA, ICE works in partnership with U.S. Customs and Border Protection and U.S. companies that manufacture, sell or export strategic technology and munitions. For more information, see <http://www.ice.gov/project-shield/> or contact ICE Headquarters, PSA Program Manager at (202) 732-3765 or (202) 732-3764.

## Trade Facilitation

### Anti-dumping Countervailing Duties Search

**(ADD/CVD)** is a searchable database of antidumping and countervailing duty messages that can be retrieved based on simple or complex search characteristics using keywords and Boolean operators. For more information, see <http://addcvd.cbp.gov/index.asp?ac=home>

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

**Automated Manifest System (AMS)** is a multi-modular cargo inventory control and release notification system. AMS facilitates the movement and delivery of cargo by multiple modes of transportation. Carriers, port authorities, service bureaus, freight forwarders, and container freight stations can participate in AMS. Sea AMS allows participants to transmit manifest data electronically prior to vessel arrival. CBP can then determine in advance whether the merchandise merits examination or immediate release. For more information about AMS, visit [http://www.cbp.gov/xp/cgov/trade/automated/automated\\_systems/ams/](http://www.cbp.gov/xp/cgov/trade/automated/automated_systems/ams/).

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

### Automated Commercial Environment (ACE)

**National Help Desk** provides customer technical support services 24 hours a day, 7 days a week, including information about ACE Secure Data Portal account access, account management, and report generation. The ACE Help Desk is the first point of contact for all ACE users experiencing system difficulties. To reach the ACE Help Desk, call (800) 927-8729.

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

**Cargo Systems Messaging Service (CSMS)** is an active, live, searchable database of messages that are of interest to Automatic Broker Interface (ABI) filers, Automated Commercial Environment (ACE) event participants, ACE Portal Accounts users, ACE reports users, air carriers, ocean carriers, Periodic Monthly Statement participants, and rail and truck carriers.

CSMS is augmented by an e-mail subscription service, which is available at:

[https://service.govdelivery.com/service/multi\\_subscribe.html?code=USDHSCBP&custom\\_id=938&origin=https://apps.cbp.gov/csms](https://service.govdelivery.com/service/multi_subscribe.html?code=USDHSCBP&custom_id=938&origin=https://apps.cbp.gov/csms).

**CBP Client Representatives** are the first points of contact for importers, exporters, transportation providers, and brokers wishing to automate any of their Customs processes. Client Representatives are the contact point for all system-related problems and questions from trade partners. For more information, see [http://www.cbp.gov/xp/cgov/trade/automated/automated\\_systems/client\\_reps.xml](http://www.cbp.gov/xp/cgov/trade/automated/automated_systems/client_reps.xml) or (571) 468-5000.

**CBP INFO Center Self Service Q&A Database** is a searchable database with over 600 answers to questions about CBP programs, requirements, and procedures. If visitors to the site are unable to find an answer to their question, they may also submit an inquiry or complaint for personal assistance. To use the searchable database, visit [https://help.cbp.gov/cgi-bin/customs.cfg/php/enduser/home.php?p\\_sid=YeyXThOj](https://help.cbp.gov/cgi-bin/customs.cfg/php/enduser/home.php?p_sid=YeyXThOj) or call the CBP INFO Center at (877) CBP-5511 or (703) 526-4200.

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

**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 <http://rulings.cbp.gov/index.asp?ac=about>

**Customs-Trade Partnership Against Terrorism (C-TPAT)** is a voluntary government-business initiative to strengthen and improve the overall international supply chain and U.S. border security. Through this initiative, businesses ensure the integrity of their security practices, communicate, and verify the security guidelines of their business partners within the supply chain. For more information, or to apply online, visit [http://www.cbp.gov/xp/cgov/trade/cargo\\_security/ctpat/](http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/). For questions or concerns, contact the CBP Industry Partnership Program at (202) 344-1180 or [industry.partnership@dhs.gov](mailto:industry.partnership@dhs.gov).

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

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

**Informed Compliance Publications** are available on a specific trade issue, which summarizes practical information for the trade community to better understand their obligations under customs and related laws. For more information, see [http://www.cbp.gov/xp/cgov/trade/legal/informed\\_compliance\\_pubs/](http://www.cbp.gov/xp/cgov/trade/legal/informed_compliance_pubs/).

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

**U.S. Border Patrol Checkpoints Brochure** provides information for the public about Border Patrol checkpoints available at: [http://www.cbp.gov/linkhandler/cgov/newsroom/fact\\_sheets/border/border\\_patrol/bp\\_checkpoints.ctt/bp\\_checkpoints.pdf](http://www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/border/border_patrol/bp_checkpoints.ctt/bp_checkpoints.pdf).

## Travel Facilitation

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

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

**Global Entry**, one of the CBP trusted traveler programs, allows pre-approved, low-risk travelers expedited clearance upon arrival into the U.S. Although this program is intended for “frequent travelers” who make several international trips per year, there is no minimum number of trips an applicant must make in order to qualify. For more information about Global Entry, visit

[www.globalentry.gov](http://www.globalentry.gov), apply online at <https://goes-app.cbp.dhs.gov/>, or contact [cbp.goes.support@dhs.gov](mailto: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. To initiate an inquiry, log onto the DHS TRIP website, [www.dhs.gov/trip](http://www.dhs.gov/trip). For more information, contact the TSA Contact Center, (866) 289-9673.

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

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

# Enforcing and Administering Our Immigration Laws

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

## Immigration Questions and Concerns

**CIS Ombudsman Annual Reports to Congress** focus on identifying systemic issues that cause delay in granting immigration benefits as well as pervasive and serious problems faced by individuals and employers in their interactions with USCIS. The Annual Report contains cumulative analysis and recommendations and provides details on activities undertaken by the Ombudsman during the reporting period of June 1 through May 31 of the calendar year. For more information, see [http://www.dhs.gov/files/publications/gc\\_1301971419354.shtm#1](http://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 [http://www.dhs.gov/xfoia/gc\\_1306427283101.shtm](http://www.dhs.gov/xfoia/gc_1306427283101.shtm).

**CIS Ombudsman's Community Call-In Teleconference Series** provides an opportunity to discuss your interactions with USCIS and share your comments, thoughts, and suggestions as well as any issues of concern. For more information, including questions and answers from previous teleconferences and a schedule of upcoming calls, visit [http://www.dhs.gov/files/programs/gc\\_1171038701035.shtm](http://www.dhs.gov/files/programs/gc_1171038701035.shtm). To participate in these calls, please RSVP to [cisombudsman.publicaffairs@dhs.gov](mailto:cisombudsman.publicaffairs@dhs.gov) specifying which call you would like to join. Participants will receive a return e-mail with the call-in information.

**Previous Recommendations by the CIS Ombudsman** are intended to ensure national security and the integrity of the legal immigration system, increase efficiencies in administering citizenship and immigration services, and improve customer service in the rendering of citizenship and immigration services. Problems reported to the Ombudsman by individuals and employers (during the Ombudsman's travels), discussions with immigration stakeholders, and suggestions of USCIS employees themselves provide the basis for many of the recommendations. [http://www.dhs.gov/files/publications/editorial\\_0769.shtm](http://www.dhs.gov/files/publications/editorial_0769.shtm)

**Send Your Recommendations to the CIS Ombudsman** Your recommendations are accepted and encouraged. The Ombudsman is dedicated to identifying systemic problems in the immigration benefits process and preparing recommendations for submission to U.S. Citizenship and Immigration Services (USCIS) for process changes. Recommendations for process changes should not only identify the problem experienced, but should also contain a proposed solution that will not only benefit an individual case, but others who may be experiencing the same problem as well. Send comments, examples, and suggestions to [cisombudsman@dhs.gov](mailto:cisombudsman@dhs.gov).

**Submit a Case Problem to the CIS Ombudsman** If you are experiencing problems during the adjudication of an immigration benefit with USCIS, you can submit a case problem to the CIS Ombudsman using DHS Form 7001 (CIS Ombudsman Case Problem Submission Form). To submit a case problem on behalf of somebody other than yourself, you should ensure that the person the case problem is

about (the applicant for a USCIS immigration benefit, or the petitioner who seeks to obtain an immigration benefit for a third party) consents to your inquiry (see Submitting a Case Problem using DHS Form 7001: Section 15 Consent). For more information, see [http://www.dhs.gov/files/programs/editorial\\_0497.shtm](http://www.dhs.gov/files/programs/editorial_0497.shtm).

## Immigration

**A Guide to Naturalization** contains information about the naturalization process, laws and regulations. See <http://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 <http://www.citizenshiptoolkit.gov>.

**USCIS Avoid Scams Resource Center** is web-based to help applicants, organizations and legal service providers understand immigration services scams and gain the necessary knowledge on seeking immigration help and how to legally provide help. For more information, see [www.uscis.gov/avoidscams](http://www.uscis.gov/avoidscams).

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

**USCIS Information for Employers and Employees** is a website regarding the employment authorization verification process and the immigration petition process. Please visit [www.uscis.gov](http://www.uscis.gov) and click on 'Information for Employers and Employees' under 'Working in the US' or click [here](#). For more information contact [Public.Engagement@dhs.gov](mailto:Public.Engagement@dhs.gov).

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

**USCIS Resources** USCIS offers a variety of resources including customer guides, videos, citizenship toolkits, an immigration law glossary, reports and studies, civics and citizenship education resources, and a historical library. See the "Resources" section at <http://www.uscis.gov>. USCIS has also made all of 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 <http://www.uscis.gov>. For more information contact [Public.Engagement@dhs.gov](mailto:Public.Engagement@dhs.gov).

**Visa Waiver Program (VWP)** enables citizens and nationals from 36 countries to travel to and enter the United States for business or visitor purposes for up to 90 days without obtaining a visa. For more information about the Visa Waiver Program, please visit

[http://www.cbp.gov/xp/cgov/travel/id\\_visa/business\\_pleasure/vwp/](http://www.cbp.gov/xp/cgov/travel/id_visa/business_pleasure/vwp/).

## Employment Eligibility Verification

**E-Verify** is a fast, free and easy to use Internet-based service that allows employers to determine the eligibility of their employees to work in the United States. E-Verify uses information provided on each employee's Form I-9, but employers must enroll in E-Verify before gaining access to the service. For most employers, enrolling in E-Verify is voluntary and only new hires must be verified using the service. To help prepare you to enroll, E-Verify provides guides, videos, webinars, and a number of other resources online in English, Spanish and other languages. You may also request an E-Verify speaker for your next event. For more information, visit [www.dhs.gov/E-Verify](http://www.dhs.gov/E-Verify) or [www.uscis.gov/Espanol/E-Verify](http://www.uscis.gov/Espanol/E-Verify), follow us on Twitter <http://twitter.com/USCIS>, [subscribe to our e-newsletter](#), [E-Verify Connection](#), or call (888) 464-4218.

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

**Form I-9**, Employment Eligibility Verification is used to verify the identity and employment authorization of each new U.S. hire. Since November 6, 1986, employers are required to complete a Form I-9 and examine documentation for each new U.S. hire. On May 13, USCIS launched I-9 Central, a new online resource center dedicated to Form I-9. 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 current Form I-9 page and the recently updated M-274 Handbook for Employers, Instructions for Completing Form I-9. USCIS also offers free webinars throughout the month about the use of Form I-9. For more information, visit [www.uscis.gov/I-9Central](http://www.uscis.gov/I-9Central), email [I-9Central@dhs.gov](mailto: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 E-Verify service offered directly to workers. Available in English and Spanish, Self Check enables individuals to enter the same information into Self Check that employers enter into E-Verify. If a problem exists with their records related 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](http://www.uscis.gov/selfcheck) or [www.uscis.gov/selfcheck/espanol](http://www.uscis.gov/selfcheck/espanol), email [verifyselfcheck@dhs.gov](mailto:verifyselfcheck@dhs.gov), or call (855) 804-0296.

**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](http://www.dhs.gov/E-Verify) or email [e-verify@dhs.gov](mailto:e-verify@dhs.gov).

## Immigration Enforcement

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

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

**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](http://www.ice.gov/image) or contact [IMAGE@dhs.gov](mailto:IMAGE@dhs.gov).

**Project CAMPUS Sentinel** is an outreach initiative established in April 2011 by ICE Homeland Security Investigations (HSI) directed toward academic institutions that are approved by HSI to enroll nonimmigrant students. The purpose of this outreach

program is to build mutual partnerships between HSI Special Agent in Charge offices and Student and Exchange Visitor Program certified institutions. This exchange will enable HSI to detect and proactively combat student visa exploitations and address inherent national security vulnerabilities. For more information, contact [CTCEU@DHS.gov](mailto:CTCEU@DHS.gov).

**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 the Department of Homeland Security (DHS), SEVP manages schools, nonimmigrant students in the F and M visa classifications, and their dependents. The Department of State manages Exchange Visitor Programs, nonimmigrant exchange visitors in the [J visa](#) classification, as well as their dependents. Both SEVP and the Department of State use the Student and Exchange Visitor Information System (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. The result is an easily accessible information system that provides timely data to the Department of State, Department of Justice, U.S. Customs and Border Protection, U.S. Citizenship and Immigration Services, and ICE. For more information, visit <http://www.ice.gov/sevis> or contact the SEVP Response Center at (703) 603-3400.

**Verification Programs Videos** are available to help employers use E-Verify in a non-discriminatory manner and in full compliance with their responsibilities under the terms of use. The videos provide invaluable information to human resources personnel. The videos, produced jointly by CRCL and USCIS are available online at [www.uscis.gov/everify](http://www.uscis.gov/everify). Written pamphlets accompany the videos and serve as

helpful desktop reminders. You may order (at no cost) the DVD videos and written pamphlets by contacting the DHS Office for Civil Rights and Civil Liberties at [crcl@dhs.gov](mailto:crcl@dhs.gov).

# Safeguarding and Securing Cyberspace

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

## Cybersecurity Assessment Tools

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

**Cybersecurity Evaluation Program (CSEP)** conducts voluntary cybersecurity assessments across all 18 CIKR sectors, within state governments and large urban areas. CSEP affords 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, visit [www.dhs.gov/xabout/structure/editorial\\_0839.shtm](http://www.dhs.gov/xabout/structure/editorial_0839.shtm) or contact [CSE@dhs.gov](mailto:CSE@dhs.gov).

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

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

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

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

## Cybersecurity Incident 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 <http://www.us-cert.gov/current/> or contact [info@us-cert.gov](mailto:info@us-cert.gov) (888) 282-0870.

**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 US 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 US 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](http://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](mailto:SandT-CyberLiaison@hq.dhs.gov).

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

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

**National Cyber Alert 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

<http://www.us-cert.gov/cas/> or contact [info@us-cert.gov](mailto:info@us-cert.gov) (888) 282-0870.

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

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

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

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

## Cybersecurity Technical Resources

**Cybersecurity Advisors (CSAs)** act as principal field liaisons in cybersecurity and provide a federal resource

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

**Cybersecurity Research and Development Center (CSRDC)** DHS S&T utilizes CSRDC to focus cyber security research and development efforts and to involve the best practices and personnel from academic, private industry, federal and national laboratories. For more information about this and other DHS S&T projects, workshop information and presentations, cybersecurity news, events and outreach information, see <http://www.cyber.st.dhs.gov/> or contact [SandT-Cyber-Liaison@hq.dhs.gov](mailto:SandT-Cyber-Liaison@hq.dhs.gov).

**Cybersecurity in the Retail Subsector Webinar** provides retail employees and managers with an overview of the cyber threats and vulnerabilities facing the industry. The webinar also reviews the types of cyber systems and infrastructure used by the retail industry and steps that retail personnel can take to address the unique vulnerabilities to those cyber resources. The webinar is available on HSIN-CS at <https://connect.hsin.gov/p78334832/>. For more information contact [CFSTeam@hq.dhs.gov](mailto:CFSTeam@hq.dhs.gov).

**Cybersecurity Public Trends and Analysis Report** provides awareness of the cyber security trends as observed by the U.S. Computer Emergency Readiness Team (US-CERT). The analysis in this report is based on incident information that has been reported to US-CERT, incidents identified by US-CERT, and public/private sector information identified when correlating and analyzing the data. For more information contact US-CERT at [info@us-cert.gov](mailto:info@us-cert.gov) (888) 282-0870.

### Control Systems Security Program (CSSP)

**Cybersecurity Training** is provided through an instructor-led introductory course for control system and IT professionals or a five-day advanced course which includes hands-on instruction in an actual control system environment. On-line introductory cybersecurity courses are also available. For more information, see [http://www.us-cert.gov/control\\_systems/cstraining.html](http://www.us-cert.gov/control_systems/cstraining.html) or contact [CSSP@dhs.gov](mailto:CSSP@dhs.gov).

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

**Critical Infrastructure Protection Cyber Security (CIP-CS)** leads efforts with public and private sector partners to promote safe, secure, and resilient U.S. cyber infrastructure. Major elements of the CIP-CS program include: managing and strengthening cyber critical infrastructure partnerships with public and private entities in order to effectively implement risk management and cybersecurity strategies; teaming with cyber critical infrastructure partners in the successful implementation of cybersecurity strategies; and promoting effective cyber communications processes with partners that result in a collaborative, coordinated approach to cyber awareness. For more information, contact CIP-CS at [ncsd\\_cipcs@hq.dhs.gov](mailto: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 <http://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 address 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](mailto: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. The Webinar is available on HSIN-CS at <https://connect.hsin.gov/p78334832/>. For more information, please contact the Commercial Facilities SSA at [CFSTeam@dhs.gov](mailto:CFSTeam@dhs.gov).

**Cybersecurity Information Products and Recommended Practices** provide current cybersecurity information resources and recommend security practices to help industry understand emerging control systems cyber security issues and mitigate vulnerabilities. This information will help users reduce their exposure and susceptibility to cyber attacks and exploits. For a complete list and access to cybersecurity information products, visit [http://www.us-cert.gov/control\\_systems/csdocuments.html](http://www.us-cert.gov/control_systems/csdocuments.html). For more information, contact [CSSP@dhs.gov](mailto:CSSP@dhs.gov).

### Domain Name System Security Extensions

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

**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 [http://www.us-cert.gov/control\\_systems/csstandards.html](http://www.us-cert.gov/control_systems/csstandards.html). For more information, contact [CSSP@dhs.gov](mailto:CSSP@dhs.gov).

**Information Technology Sector Specific Plan (IT SSP)** outlines the IT Sector security partners' joint implementation of the NIPP risk management framework. It describes an approach for identifying, assessing, prioritizing, and protecting critical IT Sector functions, establishing shared IT Sector goals and objectives, and aligning initiatives to meet them. To view the IT SSP, visit <http://www.dhs.gov/xlibrary/assets/nipp-ssp-information-tech-2010.pdf>. For more information, contact [ncsd\\_cipcs@hq.dhs.gov](mailto: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 (CARMA)—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](mailto:ncsd_cipcs@hq.dhs.gov).

#### **Network Security Information Exchange (NSIE)**

The NCS and the National Security Telecommunications Advisory Committee (NSTAC) recommended the establishment of an Industry-government partnership to reduce the vulnerability of the Nations' telecommunications systems to electronic intrusion. The NCS and NSTAC formed separate government and Industry Network Security Information Exchanges to share ideas on technologies and techniques for addressing and mitigating the risks to the public network and its supporting infrastructures. For more information, visit [http://www.ncs.gov/nstac/reports/fact\\_sheet/NSTAC\\_08.pdf](http://www.ncs.gov/nstac/reports/fact_sheet/NSTAC_08.pdf).

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

#### **The Protected Repository for the Defense of Infrastructure against Cyber Threats (PREDICT)**

facilitates the accessibility of computer and network operational data for use in cyber defense research and development through large-scale research datasets. PREDICT allows partners to pursue technical solutions to protect the public and private information infrastructure. It also provides researchers and developers with real network data to validate their technology and products before deploying them online. Within this project, the Los Angeles Network Data Exchange and Repository (LANDER), Network Traffic Data Repository to Develop Secure Information

Technology Infrastructure, Routing Topology and Network Reliability Dataset Project, and Virtual Center for Network and Security Data serve as data set collectors and hosts. The PREDICT Data Coordinating Center helps manage and coordinate the research data repository. For more information visit <https://www.predict.org> or contact [PREDICT-contact@rti.org](mailto:PREDICT-contact@rti.org).

#### **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 NPPD/IP Nuclear SSA at [NuclearSSA@hq.dhs.gov](mailto: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 NPPD/IP Chemical SSA at [ChemicalSector@hq.dhs.gov](mailto:ChemicalSector@hq.dhs.gov).

## **Software Assurance (SwA)**

**Automating Software Assurance** Under SwA sponsorship, MITRE, in collaboration with government, industry, and academic stakeholders, is improving the measurability of security through enumerating baseline security data, providing

standardized languages as means for accurately communicating the information, and encouraging sharing of this information with users by developing repositories (see Making Security Measurable: <http://buildsecurityin.us-cert.gov/swa/measurable.html>). MITRE issues electronic newsletters on the following technologies employed in automating SwA: Common Vulnerabilities and Exposures (CVE); Common Weakness Enumeration (CWE); Common Attack Pattern Enumeration and Classification (CAPEC); Open Vulnerability and Assessment Language (OVAL); and Malware Attribute Enumeration and Characterization (MAEC).

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

#### **Software Assurance (SwA) Forum and Working Group Sessions**

Four times per year, under the co-sponsorship of organizations in DHS, the Department of Defense (DoD), and the National Institute 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. 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 <https://www.vte.cert.org/vteweb/go/3719.aspx>.

**Software Assurance (SwA) Resources** To support SwA in higher education, SwA and the Software Engineering Institute (SEI) have developed Software Assurance Curriculum Materials (<https://buildsecurityin.us-cert.gov/swa/mswa.html>) which are freely available for download. This curriculum is formally recognized by the Institute of Electrical and Electronics Engineers (IEEE) and the Association for Computing Machinery (ACM). At the Forum and Working Group Sessions, SwA distributes CDs of SwA resources. Included on the CDs are guides, reports, and brochures on numerous topics such as: SwA Capability Benchmarking Documents ([https://buildsecurityin.us-cert.gov/swa/proself\\_assm.html](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/tpe\\_research.html](https://buildsecurityin.us-cert.gov/swa/tpe_research.html)); Evaluating and Mitigating Software Supply Chain Security Risk, May 2010 (<https://buildsecurityin.us-cert.gov/swa/downloads/MitigatingSWsupplyChainRisks10tn016.pdf>); and SwA Pocket Guide Series - free, downloadable documents on critical software assurance topics ([https://buildsecurityin.us-cert.gov/swa/pocket\\_guide\\_series.html](https://buildsecurityin.us-cert.gov/swa/pocket_guide_series.html)).

**Software Assurance (SwA) Email Newsletter** provides excellent updates and new information related to the SwA program. To subscribe to the newsletter, email [listproc@nist.gov](mailto: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](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)<sup>2</sup>, 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. Please visit <https://buildsecurityin.us-cert.gov/swa/webinars.html> for more information. Moreover, SwA supports online communities of interest, such as the Software Assurance Education Discussion Group on LinkedIn (<http://www.linkedin.com/groups?mostPopular=&gid=3430456>) and the Software Assurance Mega-Community ([http://www.linkedin.com/groups?home=&gid=1776555&trk=anet\\_ug\\_hm](http://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/>.

# Ensuring Resilience to Threats and Hazards

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

## Business Preparedness

**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.

**FEMA Continuity of Operations Division** supports the nations resiliency capabilities by developing and promulgating continuity directives and guidance for the Federal Executive Branch and providing continuity guidance to state, territorial, tribal, and local government jurisdictions and private sector critical infrastructure owners and operators. Additionally, the division coordinates, and participates in national, state, territorial, tribal, and local level continuity tests, training, and exercises, and facilitates the coordination of continuity efforts among federal and non-federal entities throughout the United States. For more information, visit <http://www.fema.gov/about/org/ncp/coop/index.shtml> or email [FEMA-STTLContinuity@dhs.gov](mailto:FEMA-STTLContinuity@dhs.gov).

**National Earthquake Hazards Reduction Program** FEMA created the *QuakeSmart* program 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 an actionable and scalable guidance and tools for the private sector, owners, managers, and employees about 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 <http://www.fema.gov/hazard/earthquake/> or <http://www.fema.gov/plan/prevent/earthquake/quakeSMART.shtm>.

**Public Transportation Emergency Preparedness Workshop - Connecting Communities Program** brings mass transit and passenger rail agency' security and emergency management officials together with federal, state, local, and tribal government representatives and the local law enforcement and first responder community to discuss security prevention and response efforts and ways to work together to prepare and protect their communities. The two-day workshops enable the participants to apply their knowledge and experiences to a range of security and emergency response scenarios. For more information, see <https://transit-safety.volpe.dot.gov/Training/ConnectingCommunities/EmergencyPreparedness.asp> or contact: [MassTransitSecurity@dhs.gov](mailto: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](http://www.ready.gov).

**Situational Awareness Viewer for Emergency Response & Recovery (SAVER2)** SAVER<sup>2</sup> is a web-based information sharing application that geospatially displays operationally relevant data from governmental and non-governmental partners. As the system is further developed, the agency plans to make it accessible to other trusted partners, including

operational private sector partners. The primary goals of SAVER<sup>2</sup> are to facilitate collaborative planning and expand shared situational awareness in order to improve decision-making during emergencies, national level exercises and national security events. For example, SAVER<sup>2</sup> will have the ability to show hurricane evacuation routes, which can be shared with federal, state, and local emergency management officials as well as the private sector. This information will aid decision makers when there is a need to mobilize assets and route resources, ensuring every community is supported. For more information on SAVER<sup>2</sup> see [www.fema.gov/pdf/privatesector/saver2\\_factsheet.pdf](http://www.fema.gov/pdf/privatesector/saver2_factsheet.pdf) or email [FEMA-Private-Sector@dhs.gov](mailto:FEMA-Private-Sector@dhs.gov).

**The Technical Assistance (TA) Program** builds and sustains capabilities through specific services and analytical capacities. TA is offered to a wide variety of organizations and grantees through an extensive menu of services responsive to national priorities. To best accommodate the wide variety of TA needs and deliverables, three levels of TA are provided. Level I/II services can be made available to private sector organizations and includes general information, models, templates, and samples. Level III services, available to private sector organizations that may be DHS grantees, provide onsite support via workshops and interaction between TA providers and recipients. For more information, visit [http://www.fema.gov/about/divisions/pppa\\_ta.shtml](http://www.fema.gov/about/divisions/pppa_ta.shtml) or contact (800) 368-6498 or email [FEMA-TARequest@fema.gov](mailto:FEMA-TARequest@fema.gov).

**Voluntary Private Sector Preparedness Accreditation and Certification Program (PS-Prep)** The PS-Prep Program is mandated by Title IX of the *Implementing Recommendations of the 9/11 Commission Act of*

2007. Congress directed the Department of Homeland Security (DHS) to develop and implement a voluntary program of accreditation and certification of private entities, and DHS delegated the program management to FEMA. The purpose of the PS-Prep Program is to enhance nationwide resilience in an all-hazards environment by encouraging private sector preparedness. The program uses standards adopted by DHS to promote private sector preparedness, including disaster management, emergency management and business continuity programs. In particular, it will provide a mechanism by which a private sector entity, such as a company, facility, not-for-profit corporation, hospital, stadium, university, or other organization, may be certified by an accredited third party, or by a Self Declaration of Conformity in the case of a small business, to demonstrate their conformity with one or more of the preparedness standards adopted by DHS. For more information see, [www.fema.gov/privatesectorpreparedness](http://www.fema.gov/privatesectorpreparedness).

## Emergency Communications

**Commercial Mobile Alert Service (CMAS)** is a component of the Integrated Public Alert and Warning System. It is an alert system that will have the capability to deliver relevant, timely, effective, and targeted alert messages to the public through cell phones, smartphones, pagers, and other mobile devices. This national capability will ensure more people receive Presidential, Imminent Threat, and AMBER alerts. For more information, see <http://www.cmasforum.com/> or contact [cmasforum@sra.com](mailto:cmasforum@sra.com).

**Communications Sector Specific Plan (COMM SSP)** involves the National Communications System in partnership with government and private sector communications members to ensure the Nation's communications networks and systems are secure, resilient and rapidly restored after an incident. Communications SSP is available at [http://www.dhs.gov/files/programs/gc\\_117986619](http://www.dhs.gov/files/programs/gc_117986619)

[7607.shtm](#). For more information, contact [comms\\_sector@hq.dhs.gov](mailto:comms_sector@hq.dhs.gov).

**Emergency Communications Guidance Documents and Methodologies** are stakeholder-driven guidance documents and methodologies to support emergency responders across the nation as they plan for and implement emergency communications initiatives. These resources identify and promote best practices for improving statewide governance, developing standard operating procedures, managing technology, supporting training and exercises, and encouraging use of interoperable communications. For more information, contact the Office of Emergency Communications at [oecc@hq.dhs.gov](mailto:oecc@hq.dhs.gov).

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

**Government Emergency Telecommunications Service (GETS)** provides authorized emergency response personnel with the resources to make emergency phone calls by priority queuing through the Nation's public communications networks. By calling the GETS access number and using an assigned PIN, federal, state, local and tribal leaders, first responders, and private sector emergency response

personnel receive priority queuing – allowing emergency calls to be placed ahead of routine phone traffic. The GETS website provides information on eligibility, technical assistance and administrative assistance for registering, maintaining and using GETS. For more information, see <http://gets.ncs.gov>, or contact [gets@dhs.gov](mailto:gets@dhs.gov).

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

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](mailto:OEC@hq.dhs.gov).

**National Communications System (NCS) Fiscal Year Report** provides government agencies, private sector entities and the general public a synopsis on the accomplishments of the NCS during each fiscal year. The report covers the NCS role in emergency response operations, highlights the accomplishments of the Office of the Manager branches, and publishes updates on national security and emergency preparedness communications efforts from the 24 Federal Departments and Agencies that comprise the NCS. NCS Fiscal Year reports can be found at <http://www.ncs.gov/library.html>. For more information, contact [ncsweb1@dhs.gov](mailto:ncsweb1@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, and ending in 2013. For more information, see [http://www.dhs.gov/files/publications/gc\\_1217521334397.shtm](http://www.dhs.gov/files/publications/gc_1217521334397.shtm) or contact the Office of Emergency Communications, [oeq@hq.dhs.gov](mailto:oeq@hq.dhs.gov).

**National Interoperability Field Operations Guide (NIFOG)** is a technical reference for radio technicians responsible for radios that will be used in disaster response applications, and for emergency communications. The NIFOG includes rules and regulations for use of nationwide and other interoperability channels, frequencies and channel names, and other reference material, formatted as a pocket-sized guide for radio technicians. The NIFOG can be accessed online at [http://www.dhs.gov/files/publications/gc\\_1297699887997.shtm](http://www.dhs.gov/files/publications/gc_1297699887997.shtm). For more information, contact the Office of Emergency Communications, [oeq@hq.dhs.gov](mailto:oeq@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 [http://www.ncs.gov/nstac/nstac\\_publications.html](http://www.ncs.gov/nstac/nstac_publications.html). For more information, contact [nstac1@dhs.gov](mailto:nstac1@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. See <http://www.safecomprogram.gov/grant/Default.aspx>.

**SAFECOM Program** is a public safety-driven communications program managed by the Office of Emergency Communications (OEC). SAFECOM works to build partnerships among all levels of government, linking the strategic planning and implementation needs of the emergency response community with federal, state, local, tribal, and territorial governments, to improve emergency response through more effective and efficient interoperable wireless communications. Together, DHS and the SAFECOM Executive Committee and Emergency Response Council shape emergency communications policy and standards to ensure projects are compatible, interoperable, and most importantly, meet the needs of end-users. For more information visit <http://www.dhs.gov/files/programs/safecom.shtm> or contact [SAFECOMGovernance@dhs.gov](mailto:SAFECOMGovernance@dhs.gov).

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

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

**Wireless Priority Service (WPS)** is the sister program to GETS and provides authorized emergency response personnel with the resources to make emergency wireless phone calls by priority queuing through the nation's public communications networks. Authorized WPS users – using authorized WPS wireless carriers – are granted priority service during national emergencies. Federal, state, local and tribal leaders, first responders, and private sector emergency response personnel are eligible. The WPS website provides information on eligibility, technical assistance and administrative assistance for registering, maintaining and using WPS. See <http://wps.ncs.gov>, contact [wps@dhs.gov](mailto:wps@dhs.gov).

## Emergency Responder Community

**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 <http://cdp.dhs.gov/index.html> 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 (HSIN-CS) Emergency Services Sector portal. For access and more information, contact the NPPD/IP Emergency Services Sector at [ESSTeam@hq.dhs.gov](mailto:ESSTeam@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 <http://www.fema.gov/privatesector/exercises.shtm>.

**Emergency Services Sector (ESS) Video** This is a three-minute video providing an overview of the ESS Sector. The video is appropriate for conferences and events to grow awareness and participation in sector activities. For more information, or to request materials contact the Emergency Services Sector-Specific Agency at <http://training.fema.gov/EMIWeb/IS/is860a/CIRC/emergency1.htm>.

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

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

**FEMA Emergency Management Institute Programs** offers several programs that are designed for those with emergency management responsibilities or meet the criteria specified at the website cited below. The

training is free of charge, but individuals from the private sector or contractors to state, local or tribal governments must pay their own transportation and lodging fees. EMI has an integrated training approach and encourages individuals from the private sector to participate in its courses. EMI programs include, but are not limited to, the Master Trainer Program, Master Exercise Practitioner Program, Professional Development Series, Applied Practices Series and the FEMA Higher Education Program. For more information, see <http://www.training.fema.gov/Programs/> or call (301) 447-1286.

**FEMA Learning Resource Center (LRC)** provides current information and resources on fire, emergency management and other all-hazards subjects. With its collection of more than 180,000 books, reports, periodicals, and audiovisual materials, the LRC houses the most extensive collection of fire service literature in the U.S. The LRC collection of books and research reports may also be accessed by requesting interlibrary loan through a local library. For more information see <http://www.lrc.fema.gov> or [netclrc@dhs.gov](mailto:netclrc@dhs.gov) (800) 638-1821.

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

**First Responder Communities of Practice** is an online network of vetted, active, and retired first responders, emergency response professionals and federal, state, local, or tribal homeland security officials sponsored by the DHS S&T’s First Responder Technologies (R-Tech) program. Registered members of this professional network share information, ideas, and best practices, enabling them to more efficiently

and effectively prepare for all hazards. See [www.firstresponder.gov](http://www.firstresponder.gov) or <https://communities.firstresponder.gov>.

**FirstResponder.gov** is a portal that enables federal, state, local, and tribal first responders to easily access and leverage federal web services, information on resources, products, standards, testing and evaluation, and best practices, in a collaborative environment. The portal provides first responders with information to develop or deploy technologies that would enhance homeland security. For more information, see [www.firstresponder.gov](http://www.firstresponder.gov).

**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](mailto:ESSTeam@hq.dhs.gov).

**Information Dashboard Framework** technology offers a customizable incident command interface that allows emergency response personnel to integrate data, organize and analyze inputs, display information, and update decision-making in real-time through preparedness and response applications, including the Emergency Response Support System (ERSS), the Laboratory Capacity Estimation Model (LCEM) and a Secure Egg Supply component. ERSS and LCEM enhance first responder capabilities by organizing data from authoritative sources to facilitate rapid information sharing between industry and government at the local, state, and national levels during an animal disease event. The LCEM is a pluggable component to ERSS allowing automated determination of diagnostic testing capacity estimates, supply and equipment usage, personnel requirements, and any process limitations for individual laboratories and the overall network. The Federal and State Transport eggs (FASTeggs) tool is a business continuity component of ERSS providing data on each premise to enable decision making by state animal health officials. For more information, visit <http://fazd.tamu.edu/information-analysis-systems/online-dashboard-to-enhance-decision-making-during-disease-outbreaks/>.

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

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

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

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

**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 <http://www.firstresponder.gov/Pages/Newsletter.aspx>.

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

**Video Quality in Public Safety (VQIPS)** Working Group was formed to focus on the major policy, technology, and practical uses and challenges of public safety video systems. Comprised of emergency responders, academics, federal partners, and vendors, the working group developed an end-user guide to help practitioners articulate their needs to vendors when they look to purchase or upgrade video systems. For more information, see [http://www.pscr.gov/projects/video\\_quality/video\\_about.php](http://www.pscr.gov/projects/video_quality/video_about.php). Contact [VQIPS\\_Working\\_Group@sra.com](mailto:VQIPS_Working_Group@sra.com).

**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 (HSIN-CS) Emergency Services Sector portal. For access and more information, contact the NPPD/IP Emergency Services Sector at [ESSTeam@hq.dhs.gov](mailto:ESSTeam@hq.dhs.gov).

## Personal and Community Preparedness

**Are You Ready? An In-depth Guide to Citizen Preparedness** provides a step-by-step approach to disaster preparedness by walking the reader through how to get informed about local emergency plans, how to identify hazards that affect their local area, and how to develop and maintain an emergency communications plan and disaster supplies kits. For more information see [www.fema.gov/areyouready](http://www.fema.gov/areyouready) or call (800) 480-2520 to order materials. Questions regarding the Citizen Corps program can be directed to [citizencorps@dhs.gov](mailto:citizencorps@dhs.gov).

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

**Citizen Corps Program:** Citizen Corps provides a platform for collaborative community planning and creates opportunities for individuals to volunteer to help their communities prepare for, respond to, and recover from emergencies. By fostering collaboration among all sectors of the community, citizens can participate in making their communities safer, stronger, and more resilient against the threats of terrorism, crime, and disasters of all kinds. A Citizen Corps Council is the forum where all organizations and members of the community are welcome to share ideas and learn about what to do before, during and after a disaster. One of the contributions of the more than 1,100 Citizen Corps Councils nationwide includes increased awareness through public education and training. Citizen Corps Councils on average, support four to five types of outreach to increase personal preparedness. Most Councils (70.5 percent) provide all hazard public education and training. In addition, most Councils provide education and training on essential local information such as local alerts and warnings (81.1 percent), local

sheltering (75.5 percent), local evacuation (66.3 percent), family emergency planning (90.4 percent) or local drills (64.5 percent). Citizen Corps Councils also promote a whole community approach to comprehensive emergency planning. Approximately 70 percent of Councils supported whole community planning by discussing, reviewing or providing input to key local plans such as community vulnerability/risk assessments, mitigation plans, evacuation plans and shelter plans. [www.fema.gov/citizencorps](http://www.fema.gov/citizencorps).

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

**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](http://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.

**DisabilityPreparedness.gov** is the Disability Resource Center of the Interagency Coordinating Council on Emergency Preparedness and Individuals with Disabilities (ICC). Maintained by the DHS Office for Civil Rights and Civil Liberties, this site is the main repository for information related to the activities of the ICC, including bimonthly updates regarding federal programs and services relevant to individuals with disabilities and emergency preparedness. The site also contains information to assist individuals with

disabilities in personal preparedness planning; provides emergency managers, first responders, and other disaster service providers with resources relevant to working with individuals who have disabilities; and offers tips regarding how individuals with disabilities can get involved in preparedness activities within their communities. This resource can be accessed at [www.disabilitypreparedness.gov](http://www.disabilitypreparedness.gov). For more information, contact [Disability.preparedness@dhs.gov](mailto:Disability.preparedness@dhs.gov), (202) 357-8483.

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

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

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

**FEMA Regulatory Materials** These regulations are typically open for public comment before they go into effect. The public can access the regulations that are currently in effect electronically, by selecting Title 44

from the drop down menu at <http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=%2Findex.tpl>. The public can submit and view comments submitted by other individuals at [www.regulations.gov](http://www.regulations.gov). For more information on federal agency rulemaking, visit [www.reginfo.gov](http://www.reginfo.gov) or to contact FEMA regulatory officials e-mail [FEMA-RULES@dhs.gov](mailto:FEMA-RULES@dhs.gov).

**Grants:** In FY 11, FEMA inserted new grant guidance on private sector engagement into the Homeland Security, Emergency Management and Tribal grant programs. A correlating grant supplemental specifically identifies ways that states may spend funding from these grants in support of private sector collaboration, based on actual needs communicated by states and localities that are already working proactively with the private sector. The FY12 grant supplemental ([http://www.fema.gov/pdf/government/grant/2012/fy12\\_hsgp\\_public.pdf](http://www.fema.gov/pdf/government/grant/2012/fy12_hsgp_public.pdf)) expands on the resources available to support state/local/tribal/territorial efforts to partner with the private sector in emergency management and homeland security initiatives.

**National Flood Insurance Program** focuses on flood insurance, floodplain management and flood hazard mapping. Nearly 20,000 communities across the U.S. and its territories participate in the NFIP by adopting and enforcing floodplain management ordinances to reduce future flood damage. In exchange, the NFIP makes Federally-backed flood insurance available to homeowners, renters, and business owners in these communities. For more information, see [www.floodsmart.gov](http://www.floodsmart.gov); flood insurance agents, please visit [www.agents.floodsmart.gov](http://www.agents.floodsmart.gov) or e-mail [asktheexpert@riskmapcds.com](mailto:asktheexpert@riskmapcds.com).

**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. The training is offered through the Emergency Management Institute's (EMI) Independent Study Program (ISP) and was designed in collaboration with both the

public and private sector. It is available to anyone, but particularly 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. <http://training.fema.gov/EMIWeb/IS/is660.asp>

**Public-Private Partnership Models** A growing collection of sample partnership models are posted to FEMA's website for reference and inspiration. Those seeking ideas on starting a partnership, or interested in sharing their own good practices can visit <http://www.fema.gov/privatesector/ppp.shtm>.

**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](http://www.ready.gov).

**Sample State Position Description and Toolkit** FEMA's Private Sector Division collaborated with the National Emergency Managers Association (NEMA) to distribute a letter to all of NEMA's membership, outlining tools and resources available to support private sector engagement within the state. In addition to the tools and resources listed in this section of the report to Congress, the letter included a sample position description based on existing successful state and federal positions. The template is written for any government emergency manager to adapt to his or her regional requirements, and offers a starting place for those who are just beginning or refining their outreach efforts. This information is also available on request by emailing [fema-private-sector@dhs.gov](mailto:fema-private-sector@dhs.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. Additional scenarios are planned for 2012.

<http://www.fema.gov/privatesector/exercises.shtm>

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

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

**U.S. Fire Administration (USFA Fire Prevention and Safety Campaigns)** delivers fire prevention and safety education to reduce the loss of life from fire-related hazards, particularly among the very young and older adults. The campaigns encourage Americans to practice fire safety and to protect themselves and their families from the dangers of fire. In addition, they provide dedicated support to public fire educators and the media to facilitate community outreach to targeted

audiences. For more information, visit <http://www.usfa.dhs.gov/campaigns/> or call (301) 447-1000.

**U.S. Fire Administration Publications** encourage Americans including private sector constituents to practice fire safety and protect themselves and their

families from the dangers of fire. Order online at <http://www.usfa.dhs.gov/applications/publications/> or contact the U.S Fire Administration via e-mail, [usfa-publications@dhs.gov](mailto:usfa-publications@dhs.gov) or phone, (800) 561-3356.

## Appendix A – Key Contacts

Component	Contact	E-mail	Phone
CBP	ACE Help Desk		800-927-8729
CBP	Air & Marine Operations Center (AMOC)		951-656-8000
CBP	Carrier Liaison Program	<a href="mailto:CLP@dhs.gov">CLP@dhs.gov</a>	202-344-3440
CBP	CBP INFO Center		877-CBP(227)-5511; International callers, 703-227-5511
CBP	Client Representative Office		571-468-5000
CBP	Electronic System for Travel Authorization (ESTA)		202-344-3710
CBP	Global Entry	<a href="mailto:cbp.goes.support@dhs.gov">cbp.goes.support@dhs.gov</a>	866-530-4172
CBP	Industry Partnership and Outreach Program	<a href="mailto:procurement-ipop@cbp.dhs.gov">procurement-ipop@cbp.dhs.gov</a>	202-344-1180
CBP	Intellectual Property Rights Help Desk	<a href="mailto:ipr.helpdesk@dhs.gov">ipr.helpdesk@dhs.gov</a>	562-980-3119 ext. 252
CBP	Intellectual Property Rights Policy and Programs	<a href="mailto:iprpolicyprograms@dhs.gov">iprpolicyprograms@dhs.gov</a>	
CBP	National Gang Intelligence Center		703-414-8600
CBP	Private Aircraft Travel Entry Programs	<a href="mailto:Private.Aircraft.Support@dhs.gov">Private.Aircraft.Support@dhs.gov</a>	
CBP	Secure Freight Initiative	<a href="mailto:securefreightinitiative@dhs.gov">securefreightinitiative@dhs.gov</a>	
CBP	Trusted Traveler Programs (NEXUS, SENTRI, FAST)	<a href="mailto:Cbp.goes.support@dhs.gov">Cbp.goes.support@dhs.gov</a>	
CRCL	Training	<a href="mailto:crcltraining@dhs.gov">crcltraining@dhs.gov</a>	202-357-8258
CRCL	Disability Preparedness	<a href="mailto:Disability.preparedness@dhs.gov">Disability.preparedness@dhs.gov</a>	202-357-8483
CRCL	Contact	<a href="mailto:CRCLOutreach@dhs.gov">CRCLOutreach@dhs.gov</a>	
CRCL	Complaints	<a href="mailto:crcl@dhs.gov">crcl@dhs.gov</a>	202-401-1474; 866-644-8360
DHS	Center for Faith-based & Neighborhood Partnerships	<a href="mailto:Infofbc@dhs.gov">Infofbc@dhs.gov</a>	
DHS	Homeland Security Information Network (HSIN)	<a href="mailto:hsin.helpdesk@dhs.gov">hsin.helpdesk@dhs.gov</a>	866-430-0162
DHS	Lessons Learned and information Sharing (LLIS)	<a href="mailto:feedback@llis.dhs.gov">feedback@llis.dhs.gov</a>	866-276-7001
DHS	National Information Exchange Model (NIEM) Program	<a href="mailto:NIEMPMO@NIEM.gov">NIEMPMO@NIEM.gov</a>	
DHS	Office of Public Affairs		202-282-8010
DHS	Office of Small and Disadvantaged Business Utilization		202-447-5555
DHS	Private Sector Office	<a href="mailto:Private.sector@dhs.gov">Private.sector@dhs.gov</a>	202-282-8484
DHS	Privacy Office	<a href="mailto:Privacy@dhs.gov">Privacy@dhs.gov</a>	703-235-0780
DNDO	Domestic Nuclear Detection Office	<a href="mailto:Dndo.info@dhs.gov">Dndo.info@dhs.gov</a>	

Appendix A – Key Contacts

DNDO	GRaDER® Program	<a href="mailto:GRaDER.questions@hq.dhs.gov">GRaDER.questions@hq.dhs.gov</a>	
FEMA	Center for Domestic Preparedness	<a href="mailto:Studentservices@cdpemail.dhs.gov">Studentservices@cdpemail.dhs.gov</a>	866-213-9553
FEMA	Centralized Scheduling and Information Desk	<a href="mailto:askcsid@dhs.gov">askcsid@dhs.gov</a>	800-368-6498
FEMA	Citizen Corps	<a href="mailto:citizencorps@dhs.gov">citizencorps@dhs.gov</a>	
FEMA	Community Emergency Response Teams	<a href="mailto:cert@dhs.gov">cert@dhs.gov</a>	
FEMA	Disaster Assistance		800-745-0243
FEMA	Emergency Lodging Assistance Program	<a href="mailto:femahousing@corplodging.com">femahousing@corplodging.com</a>	866-545-9865
FEMA	FEMA Emergency Management Institute		301-447-1200
FEMA	FEMA Learning Resource Center	<a href="mailto:netclrc@dhs.gov">netclrc@dhs.gov</a>	800-638-1821
FEMA	FEMA Private Sector Division	<a href="mailto:FEMA-Private-Sector@fema.dhs.gov">FEMA-Private-Sector@fema.dhs.gov</a>	
FEMA	First Responder Training	<a href="mailto:askCSID@dhs.gov">askCSID@dhs.gov</a>	800-368-6498
FEMA	Industry Liaison Support Center (contracting)		202-646-1895
FEMA	Maps Assistance Center	<a href="mailto:FEMAMapSpecialist@riskmapcds.com">FEMAMapSpecialist@riskmapcds.com</a>	877-336-2627
FEMA	National Incident Management System	<a href="mailto:FEMA-NIMS@dhs.gov">FEMA-NIMS@dhs.gov</a>	202-646-3850
FEMA	Regulations	<a href="mailto:FEMA-RULES@dhs.gov">FEMA-RULES@dhs.gov</a>	
FEMA	Small Business Program	<a href="mailto:FEMA-SB@dhs.gov">FEMA-SB@dhs.gov</a>	
FEMA	Technical Assistance Program	<a href="mailto:FEMA-TARrequest@fema.gov">FEMA-TARrequest@fema.gov</a>	800-368-6498
FEMA	Transportation Security Grant Programs	<a href="mailto:askcsid@dhs.gov">askcsid@dhs.gov</a>	800-386-6498
FEMA	U.S. Fire Administration		301-447-1000
FEMA	U.S. Fire Administration Publications	<a href="mailto:usfa-publications@dhs.gov">usfa-publications@dhs.gov</a>	800-561-3356
FLETC	CRADA Program Office	<a href="mailto:FLETC-CRADAProgramOffice@dhs.gov">FLETC-CRADAProgramOffice@dhs.gov</a>	912-267-2591
FLETC	Federal Law Enforcement Training Center Land Transportation Antiterrorist Training Program (LTATP)	<a href="mailto:FLETC-CounterterrorismDivision@dhs.gov">FLETC-CounterterrorismDivision@dhs.gov</a>	
I&A	DHS Open Source Enterprise	<a href="mailto:OSINTBranchMailbox@hq.dhs.gov">OSINTBranchMailbox@hq.dhs.gov</a>	
I&A	Office of Intelligence and Analysis Private Sector Partnership Program	<a href="mailto:I&amp;APrivateSectorCoordinator@hq.dhs.gov">I&amp;APrivateSectorCoordinator@hq.dhs.gov</a>	202-447-3517 or 202-870-6087
ICE	Victim Assistance Program		866-872-4973
ICE	Human Rights Violators and War Crimes Center	<a href="mailto:HRV.ICE@DHS.GOV">HRV.ICE@DHS.GOV</a>	
ICE	Homeland Security Investigations Tip-line	<a href="http://www.ice.gov/tips">www.ice.gov/tips</a>	866-347-2423
ICE	ICE Mutual Agreement between Government and Employers Program (IMAGE)	<a href="mailto:IMAGE@dhs.gov">IMAGE@dhs.gov</a>	202-732-3064
ICE	Forced Child Labor Program	<a href="mailto:Ice.forcedlabor@ice.dhs.gov">Ice.forcedlabor@ice.dhs.gov</a>	
ICE	National Intellectual Property Rights Coordination Center (IPR Center)	<a href="http://www.iprcenter.gov">www.iprcenter.gov</a>	866-IPR-2060 or 866-477-2060
ICE	National Emergency Management Division	<a href="mailto:#ICENEMDReporting@ice.dhs.gov">#ICENEMDReporting@ice.dhs.gov</a>	

Appendix A – Key Contacts

ICE	Privacy Office	<a href="mailto:ICEPrivacy@ice.dhs.gov">ICEPrivacy@ice.dhs.gov</a>	202-732-3300
ICE	Public Affairs	<a href="mailto:PublicAffairs.IceOfficeOf@dhs.gov">PublicAffairs.IceOfficeOf@dhs.gov</a>	202-732-4242
ICE	Student and Exchange Visitor Program (SEVP) Response Center	<a href="mailto:SEVP@DHS.gov">SEVP@DHS.gov</a>	703-603-3400
NPPD/CS&C	Control Systems Security Program (CSSP)	<a href="mailto:CSSP@dhs.gov">CSSP@dhs.gov</a>	
NPPD/CS&C	Cybersecurity Evaluation Tool	<a href="mailto:CSET@dhs.gov">CSET@dhs.gov</a>	
NPPD/CS&C	ICS-CERT Security Operations Center	<a href="mailto:ics-cert@dhs.gov">ics-cert@dhs.gov</a>	1-877-776-7585
NPPD/CS&C	Information Technology Sector	<a href="mailto:ncsd_cipcs@hq.dhs.gov">ncsd_cipcs@hq.dhs.gov</a>	
NPPD/CS&C	Office of Emergency Communications	<a href="mailto:oec@hq.dhs.gov">oec@hq.dhs.gov</a>	
NPPD/CS&C	SAFECOM Program	<a href="mailto:SAFECOMGovernance@dhs.gov">SAFECOMGovernance@dhs.gov</a>	
NPPD/CS&C	Software Assurance Program	<a href="mailto:software.assurance@dhs.gov">software.assurance@dhs.gov</a>	
NPPD/CS&C	U.S. Computer Emergency Readiness Team (US-CERT)	<a href="mailto:info@us-cert.gov">info@us-cert.gov</a>	888-282-0870
NPPD/CS&C	US-CERT Secure Operations Center	<a href="mailto:soc@us-cert.gov">soc@us-cert.gov</a>	888-282-0870
NPPD/IP	Chemical Facility Anti-Terrorism Standards (CFATS) Help Desk	<a href="mailto:CSAT@dhs.gov">CSAT@dhs.gov</a>	866-323-2957
NPPD/IP	Chemical Facility Anti-Terrorism Standards Compliance Assistance Visit Requests	<a href="mailto:CFATS@dhs.gov">CFATS@dhs.gov</a>	
NPPD/IP	Chemical Sector Specific Agency	<a href="mailto:ChemicalSector@hq.dhs.gov">ChemicalSector@hq.dhs.gov</a>	
NPPD/IP	CIKR Asset Protection Technical Assistance Program (CAPTAP)	<a href="mailto:Traininghelp@hq.dhs.gov">Traininghelp@hq.dhs.gov</a>	703-235-3939
NPPD/IP	Commercial Facilities Sector-Specific Agency	<a href="mailto:CFSteam@hq.dhs.gov">CFSteam@hq.dhs.gov</a>	
NPPD/IP	Critical Manufacturing Sector-Specific Agency	<a href="mailto:criticalmanufacturing@hq.dhs.gov">criticalmanufacturing@hq.dhs.gov</a>	
NPPD/IP	Dams Sector-Specific Agency	<a href="mailto:dams@dhs.gov">dams@dhs.gov</a>	
NPPD/IP	Emergency Services Sector-Specific Agency	<a href="mailto:ESSTeam@hq.dhs.gov">ESSTeam@hq.dhs.gov</a>	
NPPD/IP	Field Operations Branch	<a href="mailto:FOAnalysts@hq.dhs.gov">FOAnalysts@hq.dhs.gov</a>	703-235-9349
NPPD/IP	Infrastructure Data Taxonomy (IDT)	<a href="mailto:IDT@hq.dhs.gov">IDT@hq.dhs.gov</a>	
NPPD/IP	Integrated Common Analytical Viewer (iCAV)	<a href="mailto:iCAV.info@hq.dhs.gov">iCAV.info@hq.dhs.gov</a>	703-235-4949
NPPD/IP	IP Education and Learning Series	<a href="mailto:IP_Education@hq.dhs.gov">IP_Education@hq.dhs.gov</a>	
NPPD/IP	National Infrastructure Coordinating Center (NICC)	<a href="mailto:NICC@hq.dhs.gov">NICC@hq.dhs.gov</a>	202-282-9201
NPPD/IP	National Infrastructure Protection Plan (NIPP)	<a href="mailto:NIPP@dhs.gov">NIPP@dhs.gov</a>	
NPPD/IP	Nuclear Sector-Specific Agency	<a href="mailto:nuclearSSA@hq.dhs.gov">nuclearSSA@hq.dhs.gov</a>	
NPPD/IP	Office for Bombing Prevention	<a href="mailto:OBP@dhs.gov">OBP@dhs.gov</a>	
NPPD/IP	Protected Critical Infrastructure Information (PCII) Program	<a href="mailto:pcii-info@dhs.gov">pcii-info@dhs.gov</a>	202-360-3023
NPPD/IP	Sector Specific Agency Executive Management Office	<a href="mailto:SSAexecsec@dhs.gov">SSAexecsec@dhs.gov</a>	
NPPD/IP	Vulnerability Assessments Branch	<a href="mailto:IPassessments@dhs.gov">IPassessments@dhs.gov</a>	
NPPD/IP	Sector Coordinating Council	<a href="mailto:Sector.Partnership@dhs.gov">Sector.Partnership@dhs.gov</a>	

Appendix A – Key Contacts

Privacy	DHS Privacy Office		703-235-0780
S&T	Commercialization Office	<a href="mailto:SandT_Commercialization@hq.dhs.gov">SandT_Commercialization@hq.dhs.gov</a>	202-254-6749
S&T	Cyber Security Research and Development Center	<a href="mailto:SandT-Cyber-Liaison@hq.dhs.gov">SandT-Cyber-Liaison@hq.dhs.gov</a>	
S&T	Cyber Security Liaison	<a href="mailto:SandT-Cyber-Liaison@hq.dhs.gov">SandT-Cyber-Liaison@hq.dhs.gov</a>	
S&T	Office of University Programs	<a href="mailto:universityprograms@dhs.gov">universityprograms@dhs.gov</a>	202-254-5695
S&T	Project 25 Compliance Assessment Program (P25 CAP)	<a href="mailto:P25CAP@dhs.gov">P25CAP@dhs.gov</a>	
S&T	SAFETY Act	<a href="mailto:SAFETYActHelpDesk@dhs.gov">SAFETYActHelpDesk@dhs.gov</a>	866-788-9318
S&T	Small Business Innovation Program (SBIR)	<a href="mailto:stsbir.program@dhs.gov">stsbir.program@dhs.gov</a>	
TSA	Cargo Certified Cargo Screening Program	<a href="mailto:ccsp@dhs.gov">ccsp@dhs.gov</a>	
TSA	Freight and Rail	<a href="mailto:freightrailsecurity@dhs.gov">freightrailsecurity@dhs.gov</a>	
TSA	General Aviation Secure Hotline		1-866-GA-SECUR (1-866-427-3287)
TSA	Highway and Motor Carrier Division	<a href="mailto:highwaysecurity@dhs.gov">highwaysecurity@dhs.gov</a>	
TSA	Intermodal Security Training and Exercise Program (I-STEP)	<a href="mailto:i-step@dhs.gov">i-step@dhs.gov</a>	571-227-5150
TSA	Mass Transit	<a href="mailto:MassTransitSecurity@dhs.gov">MassTransitSecurity@dhs.gov</a>	
TSA	Office of Airspace Waivers		571-227-2071
TSA	Pipeline Security Division	<a href="mailto:PipelineSecurity@dhs.gov">PipelineSecurity@dhs.gov</a>	
TSA	Port & Intermodal Security Division	<a href="mailto:Maritime@dhs.gov">Maritime@dhs.gov</a>	571-227-3556
TSA	TSA Contact Center		1-866-289-9673
USCG	America's Waterway Watch	<a href="mailto:aww@uscg.mil">aww@uscg.mil</a>	202-372-1106 or 202-372-1108
USCG	Regulations	<a href="mailto:HQS-PSREGS@uscg.mil">HQS-PSREGS@uscg.mil</a>	202-372-1400
CIS Ombudsman	CIS Ombudsman	<a href="mailto:cisombudsman@dhs.gov">cisombudsman@dhs.gov</a>	
USCIS	E-Verify	<a href="mailto:E-Verify@dhs.gov">E-Verify@dhs.gov</a>	888-464-4218
USCIS	Office of Public Engagement	<a href="mailto:Public.Engagement@dhs.gov">Public.Engagement@dhs.gov</a>	
USSS	Office of Investigations		202-406-5716
USSS	Criminal Investigative Division		202-406-9330
USSS	Forensic Services Division		202-406-5926

# Appendix B – Index

## A

### Academic Engagement

- Automating Software Assurance, 49
- Cybersecurity Research and Development Center (CSRDC), 47
- Electronic Crimes Task Force (ECTF) Program, 15
- Minority Serving Institutions (MSIs) Programs, 7
- National Nuclear Forensics Expertise Development Program (NNFEDP), 34
- Project CAMPUS Sentinel, 45
- Science and Technology Directorate’s Career Development Grants (CDG) Program, 24
- The Student and Exchange Visitor Program (SEVP), 45
- Voluntary Private Sector Preparedness Accreditation and Certification Program (PS-Prep), 51

### Activity Reporting

- “If You See Something, Say Something™” Campaign, 37
- 1-800 BE ALERT, 40
- AIRBUST Program, 18
- Chemical Facility Anti-Terrorism Standards (CFATS) Chemical Facility Security Tip Line, 21
- Forced Labor Resources, 6
- General Aviation Secure Hotline, 18
- Highway and Motor Carrier First Observer™ Call-Center, 40
- Highway ISAC, 29
- Homeland Security Investigations (HSI) Tip-line, 40
- HOMEPORT, 32
- Human Rights Violators and War Crimes Center, 7
- Joint Analysis Center (JAC) Program, 34
- On the Tracks Rail Sabotage Awareness and Reporting (DVD & Poster), 30
- Report an IPR Violation, 16
- School Transportation Security Awareness (STSA), 30
- Suspicious Activity Reporting Tool, 28
- U. S. Computer Emergency Readiness Team (US-CERT) Operations Center, 47

### Advisory Council

- Area Maritime Security Committees (AMSCs), 31
- Harbor Safety Committees, 31
- Homeland Security Advisory Council (HSAC), 10
- National Infrastructure Advisory Council (NIAC), 24
- National Infrastructure Protection Plan (NIPP) Sector Partnership, 10
- National Science and Technology Council (NSTC) Subcommittee on Biometrics and Identity Management (BIDM), 38
- Sector-Specific Agency (SSA) for Communications, 11
- Telecom / Energy Working Group, 11

## B

### Bombing Prevention

- Bomb-making Materials Awareness Program (BMAP), 19
- Countering IEDs Training for Pipeline Employees, 29
- DHS Center of Excellence: Awareness & Location of Explosives-Related Threats (ALERT), 20
- Improvised Explosive Device (IED) Awareness / Bomb Threat Management Workshop, 20

- Improvised Explosive Device (IED) Counterterrorism Workshop, 20
- Improvised Explosive Device (IED) Recognition and Detection for Railroad Industry Employees Training (CD), 20
- Improvised Explosive Device (IED) Search Procedures Workshop, 20
- Multi-Jurisdiction Improvised Explosive Device (IED) Security Plan (MJIEDSP), 20
- Protective Measures Course, 20
- Technical Resource for Incident Prevention (TRIPwire), 39
- TRIPwire Community Gateway (TWCG), 21

### Border Security

- 1-800 BE ALERT, 40
- Anti-dumping Countervailing Duties Search (ADD/CVD), 41
- Border Entry Wait Times, 42
- CBP Laboratories and Scientific Services, 13
- CBP Newsroom, News Magazine and Alerts, 40
- DHS Center of Excellence: National Center for Border Security and Immigration (NCBSI), 40
- eAllegations, 40
- Entry Process into United States, 42
- Global Entry, 42
- Highway and Motor Carrier First Observer™ Call-Center, 40
- Homeland Security Investigations (HSI) Tip-line, 40
- ICE HSI National Security Investigations Division, 15
- ICE National Border Enforcement Security Task Force (BEST) Unit (NBU), 40
- National Vessel Movement Center (NVMC), 32
- Project Shield America (PSA), 40
- Secure Freight Initiative (SFI) and Importer Security Filing and additional carrier requirements (10+2), 32
- Traveler Redress Inquiry Program (DHS TRIP), 42
- U.S. Border Patrol Checkpoints Brochure, 42
- Western Hemisphere Travel Initiative (WHTI), 42

## C

### Chemical Security

- Chemical Facility Anti-Terrorism Standards (CFATS) Chemical Facility Security Tip Line, 21
- Chemical Facility Anti-Terrorism Standards (CFATS) Frequently Asked Questions, 21
- Chemical Facility Anti-Terrorism Standards (CFATS) Presentations, 21
- Chemical Facility Anti-Terrorism Standards (CFATS) Risk-Based Performance Standards (RBPS), 21
- Chemical Facility Security: Best Practice Guide for an Active Shooter Incident, 21
- Chemical Sector Classified Briefing, 22
- Chemical Sector Industrial Control Systems (ICS) Security Resource DVD, 22
- Chemical Sector Training Resources Guide, 22
- Chemical Security Analysis Center (CSAC), 21
- Chemical Security Assessment Tool (CSAT), 21
- Chemical Security Compliance Assistance Visit (CAV) Requests, 21
- Chemical Security Summit, 22
- Chemical Stockpile Emergency Preparedness Program (CSEPP), 22
- Chemical-Terrorism Vulnerability Information (CVI), 22
- Federal Motor Carrier Safety Administration: Guide to Developing an Effective Security Plan for the Highway Transportation of Hazardous Materials, 28

- Hazmat Motor Carrier Security Action Item Training (SAIT) Program, 29
- Hazmat Motor Carrier Security Self-Assessment Training Program, 29
- Hazmat Trucking Guidance: Highway Security-Sensitive Materials (HSSM) Security Action Items (SAIs), 29
- Infrastructure Protection Sector-Specific Tabletop Exercise Program (IP-SSTEP), Chemical Sector Tabletop Exercise (TTX), 22
- Monthly Chemical Sector Suspicious Activity Calls, 22
- Pipeline and Hazardous Materials Safety Administration  
Risk Management Self-Evaluation Framework (RMSEF), 29
- Pipeline Security Guidelines, 30
- Roadmap to Secure Control Systems in the Chemical Sector, 49
- Security Awareness Guide, 22
- Security Seminar & Exercise Series for Chemical Industry Stakeholders, 22
- Surveillance Detection for Law Enforcement and Security Professionals, 21
- Voluntary Chemical Assessment Tool (VCAT), 23
- Web-Based Chemical Security Awareness Training Program, 23
- Who's Who in Chemical Sector Security, 23
- Civil Rights and Civil Liberties**
- Community Roundtables, 6
- CRCL Impact Assessments, 6
- CRCL Monthly Newsletter, 6
- Environmental Justice Annual Implementation Report, 6
- Equal Employment Opportunity (EEO) Reports, 6
- E-Verify and Unfair Labor Practices, 44
- If You Have the Right to Work, Don't Let Anyone Take it Away Poster, 7
- Language Access, 7
- Minority Serving Institutions (MSIs) Programs, 7
- No te Engañes (Don't be Fooled), 7
- Posters on Common Muslim American Head Coverings, Common Sikh American Head Coverings, and the Sikh Kirpan, 7
- Privacy Impact Assessments (PIAs), 7
- Quarterly NGO Civil Rights / Civil Liberties Committee Meeting, 7
- Resources for Victims of Human Trafficking and Other Crimes, 8
- The Office of Civil Rights and Civil Liberties (CRCL) Annual Reports to Congress, 6
- Victim Assistance Program (VAP), 8
- Commercial Facilities**
- Active Threat Recognition for Retail Security Officers, 25
- DHS Lodging Video: "No Reservations: Suspicious Behavior in Hotels", 26
- DHS Retail Video: "What's in Store - Ordinary People/Extraordinary Events", 25
- DHS Sports Leagues/Public Assembly Video: "Check It! How to Check a Bag", 25
- Evacuation Planning Guide for Stadiums, 25
- Hotel and Lodging Advisory Poster, 25
- Infrastructure Protection Sector-Specific Table Top Exercise Program (SSTEP) for the Commercial Facilities Retail/Lodging Subsectors and Sports Leagues/Public Assembly Subsectors, 25
- IS-906 Workplace Security Awareness, 25
- IS-907 Active Shooter: What You Can Do, 25
- Retail and Shopping Center Advisory Poster, 26
- Risk Self-Assessment Tool for Stadiums and Arenas, Performing Art Centers, Lodging, Convention Centers, Racetracks, and Parks and Fairgrounds, 26
- Threat Detection & Reaction for Retail & Shopping Center Staff, 26
- Conference or Forum**
- Building Resilience through Public-Private Partnerships Conference, 8
- Chemical Security Summit, 22
- Community Roundtables, 6
- Critical Manufacturing Partnership Road Show, 24
- Critical Manufacturing Security Conference, 24
- Critical Manufacturing Working Groups, 8
- DHS for a Day, 9
- FEMA Think Tank, 9
- Mass Transit Security and Safety Roundtables, 33
- Private Sector for a Day, 10
- Public Transportation Emergency Preparedness Workshop - Connecting Communities Program, 51
- Quarterly NGO Civil Rights / Civil Liberties Committee Meeting, 7
- SAFECOM Guidance on Emergency Communications Grants, 53
- Software Assurance (SwA) Forum and Working Group Sessions, 49
- Technologies for Critical Incident Preparedness (TCIP) Conference and Exposition, 55
- Counterfeit Protection**
- Anti-Piracy Public Service Announcement, 15
- eInformation Network, 15
- Electronic Crimes Task Force (ECTF) Program, 15
- Financial Crimes Task Forces, 15
- HSI Illicit Finance and Proceeds of Crime Unit (IFPCU), 15
- Critical Infrastructure**
- 2011 National Sector Risk Assessment (NSRA), 11
- American National Standards Institute – Homeland Security Standards Database (ANSI-HSSD), 11
- American National Standards Institute – Homeland Security Standards Panel (ANSI-HSSP), 11
- Automated Critical Asset Management System (ACAMS) Web-Based Training, 23
- Communications Sector Specific Plan (COMM SSP), 52
- Control Systems Security Program (CSSP), 48
- Critical Infrastructure Asset Protection Technical Assistance Program (CAPTAP), 23
- Critical Infrastructure Information Notices, 36
- Critical Infrastructure Learning Series, 23
- Critical Infrastructure Protection Cyber Security (CIP-CS), 48
- Critical Infrastructure Resource Center, 23
- Critical Infrastructure Sector Snapshots, 23
- Critical Infrastructure Training Module, 23
- Cross-Sector Supply Chain Working Group (CSSCWG), 9
- Cyber Resiliency Review (CRR), 46
- Cybersecurity Evaluation Program (CSEP), 46
- Cybersecurity in the Emergency Services Sector, 54
- Daily Open Source Infrastructure Report, 36
- DHS Center of Excellence:Global Terrorism Database, 23
- DHS Center of Excellence:National Consortium for the Study of Terrorism and Responses to Terrorism (START), 24
- DHS Center of Excellence:Training Programs related to the Human Causes and Consequences of Terrorism, 23
- DHS Geospatial Information Infrastructure (GII), 37
- Enhanced Critical Infrastructure Protection (ECIP), 36
- Expert Judgment and Probability Elicitation, 24
- Guide to Critical Infrastructure Protection at the State, Regional, Local, Tribal, & Territorial Level (2008), 11
- Homeland Security Information Network (HSIN - Highway and Motor Carrier Portal), 29
- Homeland Security Information Network-Critical Sectors (HSIN-CS), 37
- INFOGRAMs, 38
- Information Sharing Snapshot, 37
- Infrastructure Data Taxonomy (IDT), 38

- Infrastructure Information Collection System (IICS), 38  
Infrastructure Protection Report Series (IPRS), 11  
Infrastructure Protection Sector-Specific Tabletop Exercise Program (IP-SSSTEP), Chemical Sector Tabletop Exercise (TTX), 22  
International Issues for Critical Infrastructure and Key Resources (CIKR) Protection, 11  
IS-821 Critical Infrastructure Support Annex, 11  
IS-860.a National Infrastructure Protection Plan (NIPP), 11  
IS-890.a Introduction to the Interagency Security Committee (ISC), 11  
National Infrastructure Advisory Council (NIAC), 24  
National Infrastructure Protection Plan (NIPP) 2009, 12  
National Infrastructure Protection Plan (NIPP) Sector Partnership, 10  
NIPP in Action Stories, 12  
NPPD/IP SOPD Critical Infrastructure Sector Snapshots, Fact Sheets and Brochures, 24  
Office of Infrastructure Protection (IP) and National Infrastructure Protection Plan (NIPP) Booths, 12  
Pipeline Security Awareness for the Pipeline Industry Employee Training CD and Brochures, 30  
Port Security Grant Program, 32  
Protected Critical Infrastructure Information (PCII) Program, 38  
Protective Security Advisors, 24  
Public Transportation Emergency Preparedness Workshop - Connecting Communities Program, 51  
Regional Resiliency Assessment Program (RRAP), 36  
Sector Annual Reports (FOUO), 12  
Sector-Specific Agency (SSA) for Communications, 11  
Sector-Specific Pandemic Influenza Guides, 28  
Sector-Specific Plans, 12  
Site Assistance Visits (SAVs), 36  
SOPD Classified Threat Briefings, 39  
Special Event and Domestic Incident Tracker (SEdit), 36  
State and Local Implementation Snapshot, 12  
Surveillance Detection Awareness on the Job, 39  
Surveillance Detection for Law Enforcement and Security Professionals, 21  
Terrorist Organization Profiles, 24  
The DHS Operations Special Events Program (SEP), 9
- Critical Manufacturing**  
Critical Manufacturing Cybersecurity Tabletop Exercise, 24  
Critical Manufacturing Partnership Road Show, 24  
Critical Manufacturing Security Conference, 24  
SOPD/TSA Joint Exercise Program, 25
- Cybersecurity**  
Automating Software Assurance, 49  
Control Systems Security Program (CSSP), 48  
Control Systems Security Program (CSSP) Cybersecurity Training, 48  
Critical Infrastructure Protection Cyber Security (CIP-CS), 48  
Critical Manufacturing Cybersecurity Tabletop Exercise, 24  
Current Cybersecurity Activity, 46  
Cyber Forensics, 47  
Cyber Investigation Section (CIS), 46  
Cyber Resiliency Review (CRR), 46  
Cybersecurity Advisors (CSAs), 47  
Cybersecurity Education and Workforce Development Program (CEWD), 48  
Cybersecurity Evaluation Program (CSEP), 46  
Cybersecurity Evaluation Tool (CSET), 46  
Cybersecurity in the Emergency Services Sector Webinar, 48  
Cybersecurity in the Retail Sector Webinar, 48  
Cybersecurity in the Retail Subsector, 47  
Cybersecurity Information Products and Recommended Practices, 48  
Cybersecurity Public Trends and Analysis Report, 47  
Cybersecurity Research and Development Center (CSRDC), 47  
Cybersecurity Vulnerability Assessments through the Control Systems Security Program (CSSP), 46  
Dams Sector Roadmap to Secure Control Systems, 26  
Dams Sector Security Awareness Guide, 27  
Defense Technology Experimental Research (DETER), 13  
Domain Name System Security Extensions (DNSSEC) Deployment Coordinating Initiative, 48  
Electronic Crimes Task Force (ECTF) Program, 15  
Financial Crimes Task Forces, 15  
Homeland Open Security Technologies, 13  
Identity Management, 37  
Industrial Control System Cybersecurity Standards and References, 48  
Industrial Control Systems (ICS) Technology Assessments, 46  
Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), 47  
Information Technology Sector Risk Assessment (ITSRA), 46  
Information Technology Sector Specific Plan (IT SSP), 48  
National Computer Forensics Institute (NCFI), 47  
National Cyber Alert System, 47  
National Vulnerability Database (NVD), 49  
Network Security Information Exchange (NSIE), 49  
Privacy Impact Assessments (PIAs), 7  
Protective Measures Handbook (FOUO), 27  
Research and Standards Integration Program (RSI), 14  
Roadmap to Enhance Cyber Systems Security in the Nuclear Sector, 49  
Roadmap to Secure Control Systems in the Chemical Sector, 49  
Sector-Specific Plans, 12  
Software Assurance (SwA) Checklist for Software Supply Chain Risk Management, 50  
Software Assurance (SwA) Email Newsletter, 50  
Software Assurance (SwA) Forum and Working Group Sessions, 49  
Software Assurance (SwA) Outreach, 50  
Software Assurance (SwA) Resources, 50  
Software Assurance Program (SwA), 49  
Support Anti-Terrorism by Fostering Effective Technologies Act (SAFETY Act), 14  
The National Cyber Security Division's (NCSA) Critical Infrastructure Protection Cyber Security (CIP CS), 48  
The Protected Repository for the Defense of Infrastructure against Cyber Threats (PREDICT), 49  
The TechSolutions Program, 14  
The Top 25 Common Weakness Enumerations (CWE), 50  
U. S. Computer Emergency Readiness Team (US-CERT) Operations Center, 47  
U.S. Computer Emergency Readiness Team (US-CERT) Monthly Activity Summary, 47  
U.S. Computer Emergency Readiness Team (US-CERT) Security Publications, 47  
U.S. Computer Emergency Readiness Team (US-CERT) Vulnerability Notes Database, 47  
Unified Incident Command and Decision Support (UICDS), 39
- D**
- Dams**  
Active and Passive Vehicle Barriers Guide, 26  
Analysis Tool, 26  
Comprehensive Facility Reports (CFR), 26

Consequence-Based Top Screen (CTS) Reference Guide, 26  
 Consequence-Based Top Screen (CTS) Tool, 26  
 Consequence-Based Top Screen Fact Sheet, 26  
 Crisis Management Handbook, 26  
 Dams Sector Tabletop Exercise Toolbox (DSTET), 27  
 Exercise Series (DSES), 27  
 IS-870 Dams Sector: Crisis Management Overview, 27  
 IS-871 Dams Sector: Security Awareness (FOUO), 27  
 IS-872 Dams Sector: Protective Measures (FOUO), 27  
 Personnel Screening Guide for Owners and Operators, 27  
 Physical Security Measures for Levees Brochure, 27  
 Protective Measures Handbook (FOUO), 27  
 Roadmap to Secure Control Systems, 26  
 Security Awareness for Levee Owners Brochure, 27, 28  
 Security Awareness Guide, 27  
 Security Awareness Handbook, 27  
 Suspicious Activity Reporting Fact Sheet, 28  
 Suspicious Activity Reporting Tool, 28  
 Waterside Barriers Guide, 27  
 Web-Based Training Fact Sheet, 27

**DHS Center of Excellence**  
 Awareness & Location of Explosives-Related Threats (ALERT), 20  
 Center for Advancing Microbial Risk Assessment (CAMRA), 28  
 Center for Maritime, Island, & Remote/Extreme Environment Security (MIREES), 31  
 Coastal Hazards Center of Excellence (CHC), 31  
 Expert Judgment and Probability Elicitation, 24  
 Global Terrorism Database, 23  
 National Center for Border Security and Immigration (NCBSI), 40  
 National Center for Food Protection and Defense (NCFPD), 28  
 National Center for Risk and Economic Analysis of Terrorism Events (CREATE), 8  
 National Center for the Study of Preparedness and Catastrophic Event Response (PACER), 56  
 National Center for Visualization and Data Analytics (CVADA), 36  
 National Center for Zoonotic and Animal Disease Defense (ZADD), 28  
 National Consortium for the Study of Terrorism and Responses to Terrorism (START), 24  
 Training Programs related to the Human Causes and Consequences of Terrorism, 23

**Doing Business with DHS**  
 CBP Industry Partnership and Outreach Program, 8  
 CBP Laboratories and Scientific Services, 13  
 Commercialization Office, 13  
 Cooperative Research and Development Agreements, 13  
 Defense Technology Experimental Research (DETER), 13  
 DHS Industry Liaisons, 9  
 DHS Small Business Innovation Research (SBIR), 13  
 DHS Technology Transfer Program, 13  
 FEMA Industry Liaison Program, 9  
 FEMA Small Business Industry Liaison Program, 9  
 FutureTECH™, 13  
 Long Range Broad Agency Announcement (LRBAA), 13  
 Office of Small and Disadvantaged Business Utilization (OSDBU), 10  
 Planning Guidelines and Design Standards (PGDS) for Checked Baggage Inspection Systems, 14  
 Project 25 Compliance Assessment Program (P25 CAP), 14  
 SECURE™ Program, 14  
 Support Anti-Terrorism by Fostering Effective Technologies Act (SAFETY Act), 14

The Acquisition Planning Forecast System (APFS), 12

## E

### Emergency Services

Center for Domestic Preparedness (CDP), 54  
 Cybersecurity in the Emergency Services Sector, 54  
 Cybersecurity in the Emergency Services Sector Webinar, 48  
 DHS Center of Excellence: National Center for the Study of Preparedness and Catastrophic Event Response (PACER), 56  
 Donations and Volunteers Information, 56  
 Emergency Communications Guidance Documents and Methodologies, 52  
 Emergency Data Exchange Language (EDXL), 52  
 Emergency Food and Shelter National Board Program, 56  
 Emergency Planning Exercises, 54  
 Emergency Services Personal Readiness Guide for Responders and Their Families, 54  
 Emergency Services Sector (ESS), 54  
 First Responder Communities of Practice, 54  
 First Responders 'Go Kit', 55  
 FirstResponder.gov, 55  
 Government Emergency Telecommunications Service (GETS), 52  
 INFOGRAMs, 38  
 Integrated Pilot Comprehensive Exercise (IPCE), 55  
 National Emergency Communications Plan (NECP), 53  
 National Interoperability Field Operations Guide (NIFOG), 53  
 Public Transportation Emergency Preparedness Workshop - Connecting Communities Program, 51  
 Responder Knowledge Base (RKB), 55  
 Situational Awareness Viewer for Emergency Response & Recovery (SAVER2), 51  
 Technologies for Critical Incident Preparedness (TCIP) Conference and Exposition, 55  
 The R-Tech Bulletin, 55  
 Unified Hazard Mitigation Assistance (HMA) Grant Programs, 57  
 Webinar: The Ready Responder Program for the Emergency Services Sector, 55  
 Wireless Priority Service (WPS), 53

### Exercise

Critical Manufacturing Cybersecurity Tabletop Exercise, 24  
 Dams Sector Exercise Series (DSES), 27  
 Dams Sector Tabletop Exercise Toolbox (DSTET), 27  
 Emergency Planning Exercises, 54  
 Infrastructure Protection Sector-Specific Table Top Exercise Program (SSTEP) for the Commercial Facilities Retail/Lodging Subsectors and Sports Leagues/Public Assembly Subsectors, 25  
 Infrastructure Protection Sector-Specific Tabletop Exercise Program (IP-SSTEP), Chemical Sector Tabletop Exercise (TTX), 22  
 Integrated Pilot Comprehensive Exercise (IPCE), 55  
 Intermodal Security Training and Exercise Program (I-STEP), 29  
 Mass Transit and Passenger Rail - Bomb Squad Response to Transportation Systems, 33  
 Self-Facilitated Tabletop Exercises, 57  
 SOPD/TSA Joint Exercise Program, 25

**F****Fraud**

- Commercial Fraud, 15
- Electronic Crimes Task Force (ECTF) Program, 15
- How to Protect Your Rights, 15
- Identity Management, 37
- Intellectual Property Rights (IPR) and Restricted Merchandise Branch, 16
- Intellectual Property Rights (IPR) e-Recordation and IPR Search, 16
- Intellectual Property Rights (IPR) Fact Sheet, 16
- Intellectual Property Rights (IPR) Help Desk, 16
- Intellectual Property Rights (IPR) Seizure Statistics, 16
- IPR Product Identification Guide, 16
- National Intellectual Property Rights Coordination Center (IPR Center), 16
- Operation Genesis, 16
- Operation Guardian, 16
- Operation In Our Sites, 16
- Report an IPR Violation, 16

**G****Grant Program**

- Freight Rail Security Grant Program, 32
- Grants, 57
- Intercity Bus Security Grant Program, 33
- Intercity Passenger Rail Grant Program, 33
- Minority Serving Institutions (MSIs) Programs, 7
- Nonprofit Security Grant Program, 24
- Port Security Grant Program, 32
- SAFECOM Guidance on Emergency Communications Grants, 53
- Science and Technology Directorate's Career Development Grants (CDG) Program, 24
- Transportation Security Grant Programs, 31
- Unified Hazard Mitigation Assistance (HMA) Grant Programs, 57

**H****Health**

- Center for Domestic Preparedness (CDP), 54
- DHS Center of Excellence:Center for Advancing Microbial Risk Assessment (CAMRA), 28
- DHS Center of Excellence:National Center for Food Protection and Defense (NCFPD), 28
- DHS Center of Excellence:National Center for Zoonotic and Animal Disease Defense (ZADD), 28
- DHS Pandemic Influenza Impact on Communications Network Study and Best Practices, 28
- Food and Agriculture Sector Criticality Assessment Tool (FASCAT), 37
- National Science and Technology Council (NSTC) Subcommittee on Biometrics and Identity Management (BiDM), 38
- Planning for 2009 H1N1 Influenza: A Preparedness Guide for Small Business, 28
- Sector-Specific Pandemic Influenza Guides, 28

**Help Desk**

- Automated Commercial Environment (ACE) National Help Desk, 41

- CBP INFO Center Self Service Q&A Database, 41
- eAllegations, 40
- Intellectual Property Rights (IPR) Help Desk, 16
- Language Access, 7
- Send Your Recommendations to the CIS Ombudsman, 43
- Submit a Case Problem to the CIS Ombudsman, 43
- Traveler Redress Inquiry Program (DHS TRIP), 42

**Human Rights Assistance**

- Blue Campaign to Combat Human Trafficking, 6
- Blue Campaign Toolkit, 6
- Forced Labor Resources, 6
- Guidance to Federal Financial Assistance Recipients Regarding Title VI Prohibition Against National Origin Discrimination Affecting Limited English Proficient Persons, 6
- Human Rights and Vulnerable Populations, 7
- Human Rights Violators and War Crimes Center, 7
- ICE HSI National Security Investigations Division, 15
- National Center for Missing and Exploited Children (NCMEC), 7
- No te Engañes (Don't be Fooled), 7
- Resources for Victims of Human Trafficking and Other Crimes, 8
- Victim Assistance Program (VAP), 8

**I****Immigration**

- Carrier Liaison Program (CLP), 45
  - CIS Ombudsman Annual Reports to Congress, 43
  - CIS Ombudsman Updates, 43
  - CIS Ombudsman's Community Call-In Teleconference Series, 43
  - Civics and Citizenship Toolkit - A Collection of Educational Resources for Immigrants, 43
  - DHS Center of Excellence: National Center for Border Security and Immigration (NCBSI), 40
  - Electronic System for Travel Authorization (ESTA), 45
  - E-Verify, 44
  - Form I-9, 44
  - ICE Mutual Agreement between Government and Employers (IMAGE), 45
  - Previous Recommendations by the CIS Ombudsman, 43
  - Project CAMPUS Sentinel, 45
  - Self Check, 44
  - Send Your Recommendations to the CIS Ombudsman, 43
  - Submit a Case Problem to the CIS Ombudsman, 43
  - The Student and Exchange Visitor Program (SEVP), 45
  - USCIS Avoid Scams Resource Center, 43
  - USCIS Citizenship Resource Center, 43
  - USCIS Information for Employers and Employees, 44
  - USCIS Office of Public Engagement (OPE), 44
  - USCIS Resources, 44
  - USCIS Social Media, 17
  - Verification Program Webinars, 44
  - Verification Programs Videos, 45
  - Visa Waiver Program (VWP), 44
- Information Sharing and Threat Brief**
- "If You See Something, Say Something™" Campaign, 37
  - Automated Critical Asset Management System (ACAMS), 36

Chemical Sector Classified Briefing, 22  
 Commercial Mobile Alert Service (CMAS), 52  
 Critical Infrastructure Information Notices, 36  
 Current Cybersecurity Activity, 46  
 Daily Open Source Infrastructure Report, 36  
 DHS Geospatial Information Infrastructure (GII), 37  
 DHS Open Source Enterprise Daily and Weekly Intelligence Reports, 37  
 Highway ISAC, 29  
 Homeland Security Information Network (HSIN), 37  
 Homeland Security Information Network-Critical Sectors (HSIN-CS), 37  
 HOMEPORT, 32  
 Identity Management, 37  
 Information Dashboard Framework, 55  
 Information Sharing Snapshot, 37  
 Infrastructure Data Taxonomy (IDT), 38  
 Infrastructure Information Collection System (IICS), 38  
 Intelligence and Analysis Private Sector Partnership Program, 38  
 Joint DHS/FBI Classified Threat and Analysis Presentations, 38  
 Monthly Chemical Sector Suspicious Activity Calls, 22  
 Monthly Unclassified Threat Briefing, 34  
 National Center for Visualization and Data Analytics (CVADA), 36  
 National Cyber Alert System, 47  
 National Science and Technology Council (NSTC) Subcommittee on Biometrics and Identity Management (BIdM), 38  
 Nuclear Sector Classified Threat Briefing, 34  
 Port Interagency Information Sharing Assessment, 32  
 Protected Critical Infrastructure Information (PCII) Program, 38  
 SOPD Classified Threat Briefings, 39  
 Surveillance Detection Awareness on the Job, 39  
 Surveillance Detection for Law Enforcement and Security Professionals, 21  
 Technical Resource for Incident Prevention (TRIPwire), 39  
 The Evolving Threat: What You Can Do Webinar, 39  
 The National Information Exchange Model (NIEM) Program, 38  
 The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI), 38  
 TSA Alert System, 39  
 U.S. Coast Guard Maritime Information eXchange (“CGMIX”), 39  
 U.S. Coast Guard Navigation Center, 32  
 Unified Incident Command and Decision Support (UICDS), 39  
 Virtual USA (vUSA), 39

**Information Technology**  
 Information Technology Sector Risk Assessment (ITSRA), 46  
 Information Technology Sector Specific Plan (IT SSP), 48

**Intellectual Property**  
 CBP Directives Pertaining to Intellectual Property Rights, 15  
 Commercial Fraud, 15  
 How to Protect Your Rights, 15  
 Intellectual Property Rights (IPR) and Restricted Merchandise Branch, 16  
 Intellectual Property Rights (IPR) Continuous Sample Bond, 16  
 Intellectual Property Rights (IPR) Enforcement: A Priority Trade Issue, 16  
 Intellectual Property Rights (IPR) e-Recordation and IPR Search, 16  
 Intellectual Property Rights (IPR) Fact Sheet, 16  
 Intellectual Property Rights (IPR) Help Desk, 16  
 Intellectual Property Rights (IPR) Seizure Statistics, 16

IPR Product Identification Guide, 16  
 National Intellectual Property Rights Coordination Center (IPR Center), 16  
 Operation Genesis, 16  
 Operation Guardian, 16  
 Operation In Our Sites, 16  
 Report an IPR Violation, 16

**Investigation**  
 Commercial Fraud, 15  
 Cyber Forensics, 47  
 Cyber Investigation Section (CIS), 46  
 Electronic Crimes Task Force (ECTF) Program, 15  
 Financial Crimes Task Forces (FCTF), 15  
 Forced Labor Resources, 6  
 Homeland Security Investigations (HSI) Tip-line, 40  
 HSI Illicit Finance and Proceeds of Crime Unit (IFPCU), 15  
 Human Rights Violators and War Crimes Center, 7  
 ICE HSI National Security Investigations Division, 15  
 ICE Mutual Agreement between Government and Employers (IMAGE), 45  
 ICE National Border Enforcement Security Task Force (BEST) Unit (NBU), 40  
 Intellectual Property Rights (IPR) Enforcement  
   A Priority Trade Issue, 16  
 Intellectual Property Rights (IPR) e-Recordation and IPR Search, 16  
 National Computer Forensics Institute (NCFI), 47  
 National Intellectual Property Rights Coordination Center (IPR Center), 16  
 Operation Genesis, 16  
 Operation Guardian, 16  
 Operation In Our Sites, 16  
 Project CAMPUS Sentinel, 45  
 Project Shield America (PSA), 40  
 Report an IPR Violation, 16  
 The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), 47  
 USCIS Avoid Scams Resource Center, 43

## L

### Library

American National Standards Institute – Homeland Security Standards Database (ANSI-HSSD), 11  
 Cargo Systems Messaging Service (CSMS), 41  
 Customs Rulings Online Search System (CROSS), 41  
 Cybersecurity Education and Workforce Development Program (CEWD), 48  
 DHS Social Media Engagement, 17  
 eInformation Network, 15  
 FEMA Learning Resource Center (LRC), 54  
 FEMA Library, 54  
 First Responder Communities of Practice, 54  
 Industrial Control System Cybersecurity Standards and References, 48  
 National Center for the Study of Preparedness and Catastrophic Event Response (PACER), 56  
 National Interstate Economic Model (NIEMO), 8  
 National Vulnerability Database (NVD), 49  
 Software Assurance (SwA) Resources, 50  
 Software Assurance Program (SwA), 49  
 Terrorist Organization Profiles, 24

The Protected Repository for the Defense of Infrastructure against Cyber Threats (PREDICT), 49  
 The Responder Knowledge Base (RKB), 55  
 Tornado Safety Initiative, 57  
 U.S. Computer Emergency Readiness Team (US-CERT) Vulnerability Notes Database, 47  
 USCIS Resources, 44

## N

### Newsletter

Anti-Piracy Public Service Announcement, 15  
 CBP's Newsroom, News Magazine and Alerts, 40  
 CIS Ombudsman Updates, 43  
 Citizen Corps E-mail Alerts, 56  
 Coast Guard Blogs and News, 17  
 Commercial Mobile Alert Service (CMAS), 52  
 CRCL Monthly Newsletter, 6  
 Critical Infrastructure Information Notices, 36  
 Daily Open Source Infrastructure Report, 36  
 DHS Social Media Engagement, 17  
 FEMA Private Sector E-alerts, 9  
 Highway ISAC, 29  
 HSI Illicit Finance and Proceeds of Crime Unit (IFPCU), 15  
 National Cyber Alert System, 47  
 Private Sector Updates, 10  
 Software Assurance (SwA) Email Newsletter, 50  
 The Blog @ Homeland Security, 17  
 The R-Tech Bulletin, 55  
 TSA Alert System, 39  
 U.S. Computer Emergency Readiness Team (US-CERT) Monthly Activity Summary, 47

### Nuclear Security

Domestic Nuclear Detection Office (DNDO), 34  
 Integrated Pilot Comprehensive Exercise (IPCE), 55  
 Joint Analysis Center (JAC) Program, 34  
 Monthly Unclassified Threat Briefing, 34  
 National Nuclear Forensics Expertise Development Program (NNFEDP), 34  
 Nuclear Sector Classified Threat Briefing, 34  
 Nuclear Sector Information Sharing Standard Operating Procedure (SOP), 35  
 Nuclear Sector Overview, 35  
 Nuclear Sector Security Awareness Guide, 35  
 Nuclear Sector Voluntary Security Programs Fact Sheet, 35  
 Open Access to ANSI N42 Series Standards, 35  
 Radiological Emergency Preparedness Program (REP), 35  
 Roadmap to Enhance Cyber Systems Security in the Nuclear Sector, 49  
 Sector-Specific Plans, 12  
 The GRaDER® Program, 34  
 Training, Exercise, and Assistance (TE&A) Program, 35  
 Who's Who in DHS Nuclear Sector Infrastructure Protection, 35

## O

### Outreach and Engagement

Acquisition Planning Forecast System (APFS), 12

American National Standards Institute – Homeland Security Standards Panel (ANSI-HSSP), 11  
 Area Committees and Area Contingency Plans (ACPs), 31  
 Building Resilience through Public-Private Partnerships Conference, 8  
 CBP Client Representatives, 41  
 CBP Industry Partnership and Outreach Program, 8  
 CBP Trade Outreach, 41  
 CIS Ombudsman's Community Call-In Teleconference Series, 43  
 Citizen Corps Program, 56  
 Commercialization Office, 13  
 Communications Sector Specific Plan (COMM SSP), 52  
 Community Roundtables, 6  
 CRCL Monthly Newsletter, 6  
 CRCL's Facebook Page, 17  
 Critical Infrastructure Protection – Cyber Security (CIP-CS), 48  
 Critical Manufacturing Partnership Road Show, 24  
 Critical Manufacturing Working Groups, 8  
 Customs-Trade Partnership Against Terrorism (C-TPAT), 42  
 Cyber Security Advisors (CSAs), 47  
 Dams Sector Tabletop Exercise Toolbox (DSTET), 27  
 DHS Center for Faith-based & Neighborhood Partnerships (CFBNP), 9  
 DHS for a Day, 9  
 DHS Industry Liaisons, 9  
 DHS Loaned Executive Program, 9  
 DHS Loaned Professor Program (via the Intergovernmental Personnel Act Mobility Program), 9  
 DHS Private Sector Office (PSO), 9  
 DHS Small Business Innovation Research (SBIR) Program, 13  
 DHS Social Media Engagement, 17  
 Domestic Nuclear Detection Office (DNDO), 34  
 Electronic Crimes Task Force (ECTF) Program, 15  
 FEMA Industry Liaison Program, 9  
 FEMA Private Sector Division Web portal, 17  
 FEMA Private Sector E-alerts, 9  
 FEMA Regulatory Materials, 56  
 FEMA Small Business Industry Liaison Program, 9  
 FEMA Think Tank, 9  
 Grants, 57  
 Guide to Implementing Privacy, 6  
 Homeland Security Advisory Council (HSAC), 10  
 Homeland Security Information Network (HSIN), 37  
 Human Rights and Vulnerable Populations, 7  
 ICE Office of Public Affairs (OPA), 10  
 Intelligence and Analysis Private Sector Partnership Program, 38  
 Mass Transit Security and Safety Roundtables, 33  
 National Earthquake Hazards Reduction Program, 51  
 National Security Telecommunications Advisory Committee (NSTAC) Recommendations, 53  
 No te Engañes (Don't be Fooled), 7  
 Nuclear Sector Information Sharing Standard Operating Procedure (SOP), 35  
 Office of Small and Disadvantaged Business Utilization (OSDBU), 10  
 Operation Genesis, 16  
 Private Sector Division/Office of External Affairs, 10  
 Private Sector for a Day, 10  
 Private Sector Representative in the National Response Coordination Center, 10  
 Private Sector Updates, 10

Protective Security Advisors, 24  
 Public Private Partnerships: An Introductory Course, 57  
 Public Transportation Emergency Preparedness Workshop - Connecting Communities Program, 51  
 Public-Private Partnership Models, 57  
 Quarterly NGO Civil Rights / Civil Liberties Committee Meeting, 7  
 Regional and Disaster Private Sector Liaisons, 10  
 SAFECOM Program, 53  
 Sample State Position Description and Toolkit, 57  
 Sector-Specific Agency (SSA) for Communications, 11  
 Security Seminar & Exercise Series for Chemical Industry Stakeholders, 22  
 Self-Facilitated Tabletop Exercises, 57  
 Software Assurance (SwA) Outreach, 50  
 Suspicious Activity Reporting Tool, 28  
 Telecom / Energy Working Group, 11  
 The Blog @ Homeland Security, 17  
 The DHS Operations Special Events Program (SEP), 9  
 The National Council of Statewide Interoperability Coordinators, 52  
 The Technical Assistance (TA) Program, 51  
 Unified Incident Command and Decision Support (UICDS), 39  
 USCIS Office of Public Engagement (OPE), 44  
 USCIS Social Media, 17  
 Verification Program Webinars, 44  
 Virtual USA (vUSA), 39  
 Voluntary Private Sector Preparedness Accreditation and Certification Program (PS-Prep), 51

**P**

**Policy Guidance**

2011 National Sector Risk Assessment (NSRA), 11  
 American National Standards Institute – Homeland Security Standards Database (ANSI-HSSD), 11  
 American National Standards Institute – Homeland Security Standards Panel (ANSI-HSSP), 11  
 FEMA Regulatory Materials, 56  
 Guide to Critical Infrastructure Protection at the State, Regional, Local, Tribal, & Territorial Level (2008), 11  
 Infrastructure Protection Report Series (IPRS), 11  
 International Issues for Critical Infrastructure and Key Resources (CIKR) Protection, 11  
 IS-821 Critical Infrastructure and Key Resources (CIKR) Support Annex, 11  
 IS-860.a National Infrastructure Protection Plan (NIPP), 11  
 IS-890.a Introduction to the Interagency Security Committee (ISC), 11  
 National Incident Management System (NIMS), 12  
 National Infrastructure Protection Plan (NIPP) 2009, 12  
 National Response Framework (NRF), 12  
 NIPP in Action Stories, 12  
 Office of Infrastructure Protection (IP) and National Infrastructure Protection Plan (NIPP) Booths, 12  
 Physical Security Criteria for Federal Facilities: An Interagency Security Committee Standard (FOUO), 12  
 Sector Annual Reports (FOUO), 12  
 Sector-Specific Plans, 12  
 State and Local Implementation Snapshot, 12

**Preparedness**

*General*  
 Citizen Corps E-mail Alerts, 56  
 Citizen Corps Program, 56

Computable General Equilibrium (CGE) Economic Analysis Model and Expanded Framework, 8  
 Emergency Planning Exercises, 54  
 FEMA Emergency Management Institute Independent Study Program, 54  
 FEMA Emergency Management Institute Programs, 54  
 FEMA Learning Resource Center (LRC), 54  
 FEMA Library, 54  
 FEMA Private Sector Division web portal, 17  
 FEMA Regulatory Materials, 56  
 Guide to Critical Infrastructure and Key Resources (CIKR) Protection at the State, Regional, Local, Tribal, & Territorial Level (2008), 11  
 Information Technology Sector Specific Plan (IT SSP), 48  
 Lessons Learned and Information Sharing (LLIS.gov), 55  
 National Incident Management System (NIMS), 12  
 National Response Framework (NRF), 12  
 National Training and Education Division (NTED), 55  
 Private Sector Representative in the National Response Coordination Center (NRCC), 10  
 Radiological Emergency Preparedness Program (REP), 35  
 Sample State Position Description and Toolkit, 57  
 The Technical Assistance (TA) Program, 51

*Mitigation*  
 Are You Ready?, 56  
 Business Continuity Planning Suite, 51  
 DHS Pandemic Influenza Impact on Communications Network Study and Best Practices, 28  
 DisabilityPreparedness.gov, 56  
 Emergency Data Exchange Language (EDXL), 52  
 Emergency Services Personal Readiness Guide for Responders and Their Families, 54  
 Evacuation Planning Guide for Stadiums, 25  
 FEMA Continuity of Operations Division, 51  
 Multi-Band Radio (MBR) Technology, 52  
 National Communications System (NCS) Fiscal Year Report, 53  
 National Earthquake Hazards Reduction Program, 51  
 National Emergency Communications Plan (NECP), 53  
 National Flood Insurance Program, 57  
 National Interoperability Field Operations Guide (NIFOG), 53  
 National Security Telecommunications Advisory Committee (NSTAC) Recommendations, 53  
 Planning for 2009 H1N1 Influenza: A Preparedness Guide for Small Business, 28  
 Ready Business, 51  
 Ready.gov, 57  
 Sector-Specific Pandemic Influenza Guides, 28  
 Unified Hazard Mitigation Assistance (HMA) Grant Programs, 57  
 Voice over Internet Protocol (VoIP) Project, 53  
 Voluntary Private Sector Preparedness Accreditation and Certification Program (PS-Prep), 51

*Prevention*  
 Customs-Trade Partnership Against Terrorism (C-TPAT), 42  
 DHS Lodging Guide: “No Reservations: Suspicious Behavior in Hotels”, 26  
 INFOGRAMs, 38  
 Public Transportation Emergency Preparedness Workshop - Connecting Communities Program, 51  
 U.S. Fire Administration (USFA Fire Prevention and Safety Campaigns), 57

*Protection*  
 Active Threat Recognition for Retail Security Officers, 25  
 Area Maritime Security Committees (AMSCs), 31  
 Automated Critical Asset Management System (ACAMS), 36  
 Chemical Stockpile Emergency Preparedness Program (CSEPP), 22

- Cybersecurity in the Emergency Services Sector, 54
- Cybersecurity in the Emergency Services Sector Webinar, 48
- Dams Sector Consequence-Based Top Screen (CTS) Reference Guide, 26
- Dams Sector Consequence-Based Top Screen (CTS) Tool, 26
- Dams Sector Security Awareness Guide, 27
- Global Supply Chain Risk Management (GSCRM) Program, 19
- Grants, 57
- INFOGRAMs, 38
- Multi-Band Radio (MBR) Technology, 52
- Multi-Jurisdiction Improvised Explosive Device (IED) Security Plan (MJIEDSP), 20
- National Earthquake Hazards Reduction Program, 51
- Protective Measures Handbook (FOUO), 27
- Recommended Security Action Items for Fixed Base Operators, 19
- SAFECOM Guidance on Emergency Communications Grants, 53
- Telecommunications Service Priority (TSP) Program, 53
- Tornado Safety Initiative, 57
- U.S. Fire Administration Publications, 58
- Video Quality in Public Safety (VQiPS), 55
- Recovery**
  - Community Emergency Response Team (CERT), 56
  - DisasterAssistance.gov, 56
  - Donations and Volunteers Information, 56
  - Emergency Food and Shelter National Board Program, 56
  - Situational Awareness Viewer for Emergency Response & Recovery (SAVER2), 51
  - Tornado Safety Initiative, 57
- Response**
  - Area Committees and Area Contingency Plans (ACPs), 31
  - Commercial Mobile Alert Service (CMAS), 52
  - Communications Sector Specific Plan (COMM SSP), 52
  - Dams Sector Crisis Management Handbook, 26
  - DHS Center of Excellence: National Center for the Study of Preparedness and Catastrophic Event Response (PACER), 56
  - Emergency Communications Guidance Documents and Methodologies, 52
  - Emergency Data Exchange Language (EDXL), 52
  - Emergency Services Sector (ESS), 54
  - First Responder Communities of Practice, 54
  - First Responders 'Go Kit', 55
  - FirstResponder.gov, 55
  - Government Emergency Telecommunications Service (GETS), 52
  - Information Dashboard Framework, 55
  - Integrated Pilot Comprehensive Exercise (IPCE), 55
  - National Emergency Communications Plan (NECP), 53
  - National Interoperability Field Operations Guide (NIFOG), 53
  - Private Sector Representative in the National Response Coordination Center (NRCC), 10
  - Public Transportation Emergency Preparedness Workshop - Connecting Communities Program, 51
  - Responder Knowledge Base (RKB), 55
  - Situational Awareness Viewer for Emergency Response & Recovery (SAVER2), 51
  - Technologies for Critical Incident Preparedness (TCIP) Conference and Exposition, 55
  - The R-Tech Bulletin, 55
  - Unified Incident Command and Decision Support (UICDS), 39
  - Virtual USA (vUSA), 39
  - Voice over Internet Protocol (VoIP) Project, 53
  - Webinar: The Ready Responder Program for the Emergency Services Sector, 55
  - Wireless Priority Service (WPS), 53
- Privacy**
  - DHS Privacy Office, 7
  - DHS Privacy Office Disclosure and Transparency, 7
  - Privacy Impact Assessments (PIAs), 7
- Product Development**
  - Cyber Security Research and Development Center (CSRDC), 47
  - Multi-Band Radio (MBR) Technology, 52
  - System Assessment and Validation for Emergency Responders (SAVER) Program, 14
  - Technologies for Critical Incident Preparedness (TCIP) Conference and Exposition, 55
  - The TechSolutions Program, 14
  - Transportation Security Laboratory (TSL), 14
  - Video Quality in Public Safety (VQiPS), 55
- Publication**
  - Air Cargo Screening Technology List-For Passenger Aircraft, 18
  - Air Cargo Watch, 18
  - Are You Ready? An In-Depth Guide to Citizen Preparedness, 56
  - Certified Cargo Screening Program, 19
  - Chemical Facility Anti-Terrorism Standards (CFATS) Frequently Asked Questions, 21
  - Chemical Facility Security: Best Practice Guide for an Active Shooter Incident, 21
  - Chemical Sector Training Resources Guide, 22
  - CIS Ombudsman Annual Reports to Congress, 43
  - Civics and Citizenship Toolkit - A Collection of Educational Resources for Immigrants, 43
  - Comprehensive Facility Reports (CFR), 26
  - Consequence-Based Top Screen Fact Sheet, 26
  - Critical Infrastructure Sector Snapshots, 23
  - Cybersecurity Information Products and Recommended Practices, 48
  - Cybersecurity Public Trends and Analysis Report, 47
  - Dams Sector Active and Passive Vehicle Barriers Guide, 26
  - Dams Sector Consequence-Based Top Screen (CTS) Reference Guide, 26
  - Dams Sector Crisis Management Handbook, 26
  - Dams Sector Personnel Screening Guide for Owners and Operators, 27
  - Dams Sector Roadmap to Secure Control Systems, 26
  - Dams Sector Security Awareness Guide, 27
  - Dams Sector Waterside Barriers Guide, 27
  - Dams Security Awareness Handbook, 27
  - Design-Basis Threat: An Interagency Security Committee Report (FOUO), 36
  - DHS Geospatial Information Infrastructure (GII), 37
  - DHS Open Source Enterprise Daily and Weekly Intelligence Reports, 37
  - DHS Pandemic Influenza Impact on Communications Network Study and Best Practices, 28
  - Emergency Services Personal Readiness Guide for Responders and Their Families, 54
  - Entry Process into United States, 42
  - Environmental Justice Annual Implementation Report, 6
  - Equal Employment Opportunity (EEO) Reports, 6
  - Federal Motor Carrier Safety Administration: Guide to Developing an Effective Security Plan for the Highway Transportation of Hazardous Materials, 28
  - General Aviation Security Guidelines, 19
  - Guide to Critical Infrastructure and Key Resources (CIKR) Protection at the State, Regional, Local, Tribal, & Territorial Level, 11
  - Guide to Implementing Privacy, 6
  - Guide to Naturalization, 43
  - Hazmat Trucking Guidance: Highway Security-Sensitive Materials (HSSM) Security Action Items (SAIs), 29

Hotel and Lodging Advisory Poster, 25  
 If You Have the Right to Work, Don't Let Anyone Take it Away Poster, 7  
 Informed Compliance Publications, 42  
 Infrastructure Protection Report Series (IPRS), 11  
 Intellectual Property Rights (IPR) Enforcement: A Priority Trade Issue, 16  
 Intellectual Property Rights (IPR) Fact Sheet, 16  
 Intellectual Property Rights (IPR) Seizure Statistics, 16  
 International Issues for Critical Infrastructure and Key Resources (CIKR) Protection, 11  
 IPR Product Identification Guide, 16  
 Keep the Nation's Railroad Secure (Brochure), 33  
 Laminated Security Awareness Driver Tip Card, 30  
 Mass Transit Employee Vigilance Campaign, 33  
 Mass Transit Smart Security Practices, 33  
 Motorcoach Guidance: Security and Emergency Preparedness Plan (SEPP), 34  
 National Infrastructure Protection Plan (NIPP) 2009, 12  
 NPPD/IP SOPD Critical Infrastructure Sector Snapshots, Fact Sheets and Brochures, 24  
 Nuclear Sector Information Sharing Standard Operating Procedure (SOP), 35  
 Nuclear Sector Overview, 35  
 Nuclear Sector Security Awareness Guide, 35  
 Nuclear Sector Voluntary Security Programs Fact Sheet, 35  
 Office of Infrastructure Protection (IP) and National Infrastructure Protection Plan (NIPP) Booths, 12  
 Open Access to ANSI N42 Series Standards, 35  
 Physical Security Criteria for Federal Facilities: An Interagency Security Committee Standard (FOUO), 12  
 Physical Security Measures for Levees Brochure, 27  
 Posters on Common Muslim American Head Coverings, Common Sikh American Head Coverings, and the Sikh Kirpan, 7  
 Previous Recommendations by the CIS Ombudsman, 43  
 Protective Measures Handbook (FOUO), 27  
 Rail Security Rule Overview, 34  
 Retail and Shopping Center Advisory Poster, 26  
 Safeguarding America's Transportation System Security Guides, 30  
 Sector Annual Reports (FOUO), 12  
 Sector-Specific Pandemic Influenza Guides, 28  
 Security Awareness for Levee Owners Brochure, 27, 28  
 Security Awareness Guide, 22  
 Software Assurance (SwA) Checklist for Software Supply Chain Risk Management, 50  
 Suspicious Activity Reporting Fact Sheet, 28  
 The Coast Guard Journal of Safety at Sea, 31  
 The Office of Civil Rights and Civil Liberties (CRCL) Annual Reports to Congress, 6  
 The Top 25 Common Weakness Enumerations (CWE), 50  
 Trade Trends, 42  
 Transit Agency Security and Emergency Management Protective Measures, 30  
 Transportation Sector Network Management Highway and Motor Carrier Division Annual Report, 31  
 Transportation Security Administration Counterterrorism Guides, 31  
 U.S. Border Patrol Checkpoints Brochure, 42  
 U.S. Computer Emergency Readiness Team (US-CERT) Security Publications, 47  
 U.S. Fire Administration Publications, 58  
 User's Guide on Security Seals for Domestic Cargo, 19  
 Web-Based Training Fact Sheet, 27  
 Who's Who in Chemical Sector Security, 23  
 Who's Who in DHS Nuclear Sector Infrastructure Protection, 35

## R

### Research Tool

CBP Laboratories and Scientific Services, 13  
 Commercialization Office, 13  
 Cooperative Research and Development Agreements (CRADAs), 13  
 Critical Infrastructure Resource Center, 23  
 Cyber Security Research and Development Center (CSRDC), 47  
 Defense Technology Experimental Research (DETER), 13  
 DHS Small Business Innovation Research (SBIR) Program, 13  
 DHS Technology Transfer Program, 13  
 FEMA Learning Resource Center (LRC), 54  
 FEMA Library, 54  
 FutureTECH™, 13  
 Homeland Open Security Technologies, 13  
 Long Range Broad Agency Announcement (LRBAA), 13  
 Mass Transit Security Technology, 13  
 National Urban Security Technology Laboratory, 13  
 Planning Guidelines and Design Standards (PGDS) for Checked Baggage Inspection Systems, 14  
 Project 25 Compliance Assessment Program, 14  
 Research and Standards Integration Program (RSI), 14  
 SAFECOM Program, 53  
 Science & Technology Basic Research Focus Areas, 14  
 SECURE™ Program, 14  
 Support Anti-Terrorism by Fostering Effective Technologies Act (SAFETY Act), 14  
 System Assessment and Validation for Emergency Responders (SAVER) Program, 14  
 The TechSolutions Program, 14  
 Transportation Security Laboratory (TSL), 14

### Risk Assessment

#### In-person

Comprehensive Security Assessments and Action Items, 35  
 Cybersecurity Vulnerability Assessments through the Control Systems Security Program (CSSP), 46  
 Enhanced Critical Infrastructure Protection (ECIP) Visits, 36  
 Port Interagency Information Sharing Assessment, 32  
 Regional Resiliency Assessment Program (RRAP), 36  
 Site Assistance Visits (SAVs), 36

#### Web

2011 National Sector Risk Assessment (NSRA), 11  
 Chemical Facility Anti-Terrorism Standards (CFATS) Risk-Based Performance Standards (RBPS), 21  
 Chemical Security Analysis Center (CSAC), 21  
 Chemical Security Assessment Tool (CSAT), 21  
 Chemical Security Compliance Assistance Visit (CAV) Requests, 21  
 Computable General Equilibrium (CGE) Economic Analysis Model and Expanded Framework, 8  
 Computer Based Assessment Tool (CBAT), 35  
 Cyber Resiliency Review (CRR), 46  
 Cyber Security Evaluation Program (CSEP), 46  
 Cyber Security Evaluation Tool (CSET), 46  
 Dams Sector Analysis Tool, 26  
 Design-Basis Threat (DBT): An Interagency Security Committee Report (FOUO), 36  
 Expert Judgment and Probability Elicitation, 24  
 Food and Agriculture Sector Criticality Assessment Tool (FASCAT), 37  
 Hazmat Motor Carrier Security Self-Assessment Training Program, 29

HS-ANALISER: Homeland Security Analysis, modeLing, Integrated, Secured Environment and Repository for Decision Support, 36  
 Importer Self Assessment – Product Safety Pilot (ISA-PS), 42  
 Importer Self-Assessment Program (ISA), 42  
 Industrial Control Systems Technology Assessments, 46  
 Information Technology Sector Risk Assessment (ITSRA), 46  
 Mass Transit and Passenger Rail - Field Operational Risk and Criticality Evaluation (FORCE), 33  
 Multi-Jurisdiction Improvised Explosive Device (IED) Security Plan (MJIEDSP), 20  
 National Center for Risk and Economic Analysis of Terrorism Events (CREATE), 8  
 National Vulnerability Database (NVD), 49  
 Network Security Information Exchange (NSIE), 49  
 Pipeline and Hazardous Materials Safety Administration: Risk Management Self-Evaluation Framework (RMSEF), 29  
 Risk Self-Assessment Tool for Stadiums and Arenas, Performing Art Centers, Lodging, Convention Centers, Racetracks, and Parks and Fairgrounds, 26  
 Software Assurance (SwA) Checklist for Software Supply Chain Risk Management, 50  
 Special Event and Domestic Incident Tracker (SEDIT), 36  
 The National Cyber Security Division's (NCS) Critical Infrastructure Protection Cyber Security (CIP CS), 48  
 Tornado Safety Initiative, 57  
 Voluntary Chemical Assessment Tool (VCAT), 23

## S

### Supply Chain

Air Cargo Screening Technology List-For Passenger Aircraft, 18  
 Automated Commercial Environment (ACE), 41  
 Automated Commercial Environment (ACE) National Help Desk, 41  
 Automated Commercial System (ACS), 41  
 Automated Export System (AES), 41  
 Automated Manifest System (AMS), 41  
 Cargo Systems Messaging Service (CSMS), 41  
 CBP Client Representatives, 41  
 Certified Cargo Screening Program, 19  
 Customs-Trade Partnership Against Terrorism (C-TPAT), 42  
 DHS Center of Excellence: National Transportation Security Center of Excellence (NTSCOE), 29  
 Federal Motor Carrier Safety Administration: Guide to Developing an Effective Security Plan for the Highway Transportation of Hazardous Materials, 28  
 First Observer™ Training, 29  
 Freight Rail Security Grant Program, 32  
 Global Supply Chain Risk Management (GSCRM) Program, 19  
 Hazmat Motor Carrier Security Action Item Training (SAIT) Program, 29  
 Hazmat Motor Carrier Security Self-Assessment Training Program, 29  
 Hazmat Trucking Guidance: Highway Security-Sensitive Materials (HSSM) Security Action Items (SAIs), 29  
 Highway and Motor Carrier Awareness Posters, 29  
 Highway and Motor Carrier First Observer™ Call-Center, 40  
 Highway ISAC, 29  
 Homeland Security Information Network (HSIN) – Freight Rail Portal, 33  
 Homeland Security Information Network (HSIN) - Highway and Motor Carrier Portal, 29  
 Intermodal Security Training and Exercise Program (I-STEP), 29  
 Keep the Nation's Railroad Secure Brochure, 33  
 Laminated Security Awareness Driver Tip Card, 30

Land Transportation Antiterrorism Training Program (LTATP), 30  
 National Vessel Movement Center (NVMC), 32  
 Pipeline and Hazardous Materials Safety Administration  
 Risk Management Self-Evaluation Framework (RMSEF), 29  
 Rail Security Rule Overview, 34  
 Secure Freight Initiative (SFI) and Importer Security Filing and additional carrier requirements (10+2), 32  
 Software Assurance (SwA) Checklist for Software Supply Chain Risk Management, 50  
 Transportation Sector Network Management Highway and Motor Carrier Division Annual Report, 31  
 TSA Counterterrorism Guides, 31  
 U.S. Border Patrol Checkpoints Brochure, 42  
 User's Guide on Security Seals for Domestic Cargo, 19

## T

### Trade Facilitation

Anti-dumping Countervailing Duties Search (ADD/CVD), 41  
 Automated Commercial Environment (ACE), 41  
 Automated Commercial Environment (ACE) National Help Desk, 41  
 Automated Commercial System (ACS), 41  
 Automated Export System (AES), 41  
 Automated Manifest System (AMS), 41  
 Cargo Systems Messaging Service (CSMS), 41  
 CBP Client Representatives, 41  
 CBP Directives Pertaining to Intellectual Property Rights, 15  
 CBP INFO Center Self Service Q&A Database, 41  
 CBP Trade Outreach, 41  
 Customs Rulings Online Search System (CROSS), 41  
 Customs-Trade Partnership Against Terrorism (C-TPAT), 42  
 Importer Self Assessment – Product Safety Pilot (ISA-PS), 42  
 Importer Self-Assessment Program (ISA), 42  
 Informed Compliance Publications, 42  
 Trade Trends, 42

### Training

*Independent Study*  
 FEMA Emergency Management Institute Independent Study Program, 54  
 IS-821 Critical Infrastructure and Key Resources (CIKR) Support Annex, 11  
 IS-860.a National Infrastructure Protection Plan (NIPP), 11  
 IS-870 Dams Sector: Crisis Management Overview, 27  
 IS-871 Dams Sector: Security Awareness (FOUO), 27  
 IS-872 Dams Sector: Protective Measures (FOUO), 27  
 IS-890.a Introduction to the Interagency Security Committee (ISC), 11  
 IS-906 Workplace Security Awareness, 25  
 IS-907 Active Shooter: What You Can Do, 25  
*In-person*  
 Aviation Safety & Security Program, 18  
 Center for Domestic Preparedness (CDP), 54  
 Chemical Facility Anti-Terrorism Standards (CFATS) Presentations, 21  
 Control Systems Security Program (CSSP) Cybersecurity Training, 48  
 Critical Infrastructure and Key Resource (CIKR) Asset Protection Technical Assistance Program (CAPTAP), 23  
 Critical Manufacturing Partnership Road Show, 24  
 Critical Manufacturing Security Conference, 24

- FEMA Emergency Management Institute Programs, 54
- Improvised Explosive Device (IED) Awareness / Bomb Threat Management Workshop, 20
- Improvised Explosive Device (IED) Counterterrorism Workshop, 20
- Improvised Explosive Device (IED) Search Procedures Workshop, 20
- Land Transportation Antiterrorism Training Program (LTATP), 30
- National Training and Education Division (NTED), 55
- Protective Measures Course, 20
- Surveillance Detection for Law Enforcement and Security Professionals, 21
- The National Information Exchange Model (NIEM) Program, 38
- Training Programs related to the Human Causes and Consequences of Terrorism, 23
- Victim Assistance Program (VAP), 8
- Video**
  - Active Threat Recognition for Retail Security Officers, 25
  - Chemical Sector Industrial Control Systems (ICS) Security Resource DVD, 22
  - Countering IEDs Training for Pipeline Employees, 29
  - DHS Retail Video: "What's in Store - Ordinary People/Extraordinary Events", 25
  - Emergency Services Sector (ESS) Video, 54
  - E-Verify and Unfair Labor Practices Training, 44
  - First Responders 'Go Kit', 55
  - Improvised Explosive Device (IED) Recognition and Detection for Railroad Industry Employees Training (CD), 20
  - Introduction to Arab American and Muslim American Cultures, 7
  - On the Tracks Rail Sabotage Awareness and Reporting (DVD & Poster), 30
  - Operation Secure Transport (OST), 30
  - Pipeline Security Awareness for the Pipeline Industry Employee Training CD and Brochures, 30
  - Protecting Pipeline Infrastructure: The Law Enforcement Role, 30
  - Threat Detection & Reaction for Retail & Shopping Center Staff, 26
  - Verification Programs and Videos, 45
  - Video Quality in Public Safety (VQiPS), 55
  - Webinar: The Ready Responder Program for the Emergency Services Sector, 55
- Web**
  - Airport Watch/AOPA Training, 18
  - Alien Flight/Flight School Training, 18
  - Automated Critical Asset Management System (ACAMS) Web-based Training, 23
  - Blue Campaign Toolkit, 6
  - Bomb-making Materials Awareness Program (BMAP), 19
  - Carrier Liaison Program (CLP), 45
  - Chemical Sector Training Resources Guide, 22
  - Control Systems Security Program (CSSP) Cybersecurity Training, 48
  - Critical Infrastructure and Key Resources (CIKR) Training Module, 23
  - Critical Infrastructure Learning Series, 23
  - Cybersecurity Education and Workforce Development Program (CEWD), 48
  - Cybersecurity in the Emergency Services Sector, 54
  - Cybersecurity in the Emergency Services Sector Webinar, 48
  - Cybersecurity in the Retail Sector Webinar, 48
  - Cybersecurity in the Retail Subsector Webinar, 47
  - DHS Lodging Video: "No Reservations: Suspicious Behavior in Hotels", 26
  - DHS Sports Leagues/Public Assembly Video: "Check It! How to Check a Bag", 25
  - FEMA Learning Resource Center (LRC), 54
  - First Observer™ Training, 29
  - Hazmat Motor Carrier Security Action Item Training (SAIT) Program, 29
  - Hazmat Motor Carrier Security Self-Assessment Training Program, 29
  - ICE Mutual Agreement between Government and Employers (IMAGE), 45
  - Improvised Explosive Device (IED) Threat Awareness and Detection, 20
  - Intermodal Security Training and Exercise Program (I-STEP), 29
  - Maritime Passenger Security Courses, 32
  - Mass Transit Security Training Program Guidelines, 33
  - National Training and Education Division (NTED), 55
  - NIPP in Action Stories, 12
  - Pipeline and Hazardous Materials Safety Administration: Risk Management Self-Evaluation Framework (RMSEF), 29
  - Public Private Partnerships: An Introductory Course, 57
  - Public-Private Partnership Models, 57
  - Radiological Emergency Preparedness Program (REP), 35
  - School Transportation Security Awareness (STSA), 30
  - Software Assurance (SwA) Outreach, 50
  - Surveillance Detection Awareness on the Job, 39
  - The Evolving Threat: What You Can Do Webinar, 39
  - Training, Exercise, and Assistance (TE&A) Program, 35
  - TRIPwire Community Gateway (TWCG), 21
  - USCIS Citizenship Resource Center, 43
  - Voluntary Private Sector Preparedness Accreditation and Certification Program (PS-Prep), 51
  - Web-Based Chemical Security Awareness Training Program, 23
- Transportation Security**
  - Air**
    - Air Cargo Screening Technology List-For Passenger Aircraft, 18
    - Air Cargo Watch, 18
    - AIRBUST Program, 18
    - Airport Watch/AOPA Training, 18
    - Airspace Waivers, 18
    - Alien Flight/Flight School Training, 18
    - Aviation Safety & Security Program, 18
    - Certified Cargo Screening Program, 19
    - General Aviation Maryland Three Program, 19
    - General Aviation Secure Hotline, 18
    - General Aviation Security Guidelines, 19
    - Global Supply Chain Risk Management (GSCRM) Program, 19
    - Paperless Boarding Pass Pilot, 19
    - Planning Guidelines and Design Standards (PGDS) for Checked Baggage Inspection Systems, 14
    - Private Aircraft Travel Entry Programs, 19
    - Recommended General Aviation Security Action Items for General Aviation Aircraft Operators and Recommended Security Action Items for Fixed Base Operators, 19
    - Secure Flight, 19
    - User's Guide on Security Seals for Domestic Cargo, 19
  - Intermodal**
    - Intermodal Security Training and Exercise Program (I-STEP), 29
    - Sector-Specific Plans, 12
    - SOPD/TSA Joint Exercise Program, 25
    - Transportation Security Laboratory (TSL), 14
    - Traveler Redress Inquiry Program (DHS TRIP), 42
    - Trusted Traveler Programs (TTP), 42
  - Land**
    - Border Entry Wait Times, 42
    - Comprehensive Security Assessments and Action Items, 35
    - Countering IEDs Training for Pipeline Employees, 29
    - DHS Center of Excellence: National Transportation Security Center of Excellence (NTSCOE), 29

- Federal Motor Carrier Safety Administration: Guide to Developing an Effective Security Plan for the Highway Transportation of Hazardous Materials, 28
- First Observer™ Training, 29
- Freight Rail Security Grant Program, 32
- Hazmat Motor Carrier Security Action Item Training (SAIT) Program, 29
- Hazmat Motor Carrier Security Self-Assessment Training Program, 29
- Hazmat Trucking Guidance: Highway Security-Sensitive Materials (HSSM) Security Action Items (SAIs), 29
- Highway and Motor Carrier Awareness Posters, 29
- Highway and Motor Carrier First Observer™ Call-Center, 40
- Highway ISAC, 29
- Homeland Security Information Network – Public Transit Portal (HSIN-PT), 33
- Homeland Security Information Network (HSIN) – Freight Rail Portal, 33
- Homeland Security Information Network (HSIN) - Highway and Motor Carrier Portal, 29
- Improvised Explosive Device (IED) Recognition and Detection for Railroad Industry Employees Training (CD), 20
- Intercity Bus Security Grant Program, 33
- Intercity Passenger Rail Grant Program, 33
- Joint DHS/FBI Classified Threat and Analysis Presentations, 38
- Keep the Nation’s Railroad Secure Brochure, 33
- Laminated Security Awareness Driver Tip Card, 30
- Land Transportation Antiterrorism Training Program (LTATP), 30
- Mass Transit and Passenger Rail - Bomb Squad Response to Transportation Systems, 33
- Mass Transit and Passenger Rail - Field Operational Risk and Criticality Evaluation (FORCE), 33
- Mass Transit Employee Vigilance Campaign, 33
- Mass Transit Security and Safety Roundtables, 33
- Mass Transit Security Technology, 13
- Mass Transit Security Training Program Guidelines, 33
- Mass Transit Smart Security Practices, 33
- Motorcoach Guidance: Security and Emergency Preparedness Plan (SEPP), 34
- On the Tracks Rail Sabotage Awareness and Reporting (DVD & Poster), 30
- Operation Secure Transport (OST), 30
- Pipeline and Hazardous Materials Safety Administration  
Risk Management Self-Evaluation Framework (RMSEF), 29
- Pipeline Security Awareness for the Pipeline Industry Employee Training CD and Brochures, 30
- Pipeline Security Guidelines, 30
- Protecting Pipeline Infrastructure: The Law Enforcement Role, 30
- Public Transportation Emergency Preparedness Workshop - Connecting Communities Program, 51
- Rail Security Rule Overview, 34
- Safeguarding America’s Transportation System Security Guides, 30
- School Transportation Security Awareness (STSA), 30
- Transit Agency Security and Emergency Management Protective Measures, 30
- Transportation Sector Network Management Highway and Motor Carrier Division Annual Report, 31
- Transportation Security Grant Program (TSGP), 31
- TSA Alert System, 39
- TSA Counterterrorism Guides, 31
- Sea**
- America’s Waterways Watch, 31
- Area Committees and Area Contingency Plans (ACPs), 31
- Area Maritime Security Committees (AMSCs), 31
- Center for Maritime, Island, & Remote/Extreme Environment Security (MIREES), 31
- Coast Guard Blogs and News, 17
- Coastal Hazards Center of Excellence (CHC), 31
- Harbor Safety Committees, 31
- HOMEPORT, 32
- Maritime Passenger Security Courses, 32
- National Vessel Movement Center (NVMC), 32
- Port Interagency Information Sharing Assessment, 32
- Port Security Grant Program, 32
- Secure Freight Initiative (SFI) and Importer Security Filing and additional carrier requirements (10+2), 32
- The Coast Guard Journal of Safety at Sea, 31
- Transportation Worker Identification Credential (TWIC), 32
- U.S. Coast Guard Auxiliary, 32
- U.S. Coast Guard Maritime Information eXchange (“CGMIX”), 39
- U.S. Coast Guard National Maritime Center (NMC), 32
- U.S. Coast Guard Navigation Center, 32
- Vessel Documentation (for US Flag Vessels), 32
- Travel Facilitation**
- Border Entry Wait Times, 42
- Electronic System for Travel Authorization (ESTA), 45
- Entry Process into United States, 42
- Global Entry, 42
- Traveler Redress Inquiry Program (DHS TRIP), 42
- Trusted Traveler Programs (TTP), 42
- Visa Waiver Program (VWP), 44
- Western Hemisphere Travel Initiative (WHTI), 42