Science & Technology Directorate (S&T)

The S&T Directorate's mission is to improve homeland security by providing to customers state-of-the-art technology that helps them achieve their missions. S&T customers include the operating components of the Department, State, local, Tribal and territorial emergency responders and officials. www.dhs.gov/scienceandtechnology

S&T Programs

S&T Collaboration in Data and Visual Analytics both internally within the DHS research community as well as externally enables S&T to leverage both its funding and technical expertise by taking advantage of research activities underway in government laboratories, industry laboratories, and in universities across the world. In 2008, S&T's Command, Control, and Interoperability Division (CCI) established a five-year joint program with the National Science Foundation (NSF) on the Foundations of Visual and Data Analytics. In 2009, CCI contributions were matched more than twofold by NSF, and 16 universities have been awarded research grants. Additionally, DHS has signed formal international collaboration agreements between Canada, Germany and the United Kingdom, discussions with France are underway and will be formalized this year. These efforts have resulted in the development of joint scientific and technical projects in visualization and data analytics. For more information, contact iVAC@dhs.gov.

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

American National Standards Institute – Homeland Security Standards Database's (ANSI-HSSD) goal is to provide a single, comprehensive source for standards that relate to homeland security. To meet this goal, ANSI partnered with the U.S. Department of Homeland Security, 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. See www.hsd.us/ or contact Karen Hughes, Director, Homeland Security Standards, ANSI (khughes@ansi.org).

Commercial Mobile Alert Service (CMAS) is a component of the Integrated Public Alert and Warning System. It is an alert system that will have the capability to deliver relevant, timely, effective, and targeted alert messages to the public through cell phones, blackberries, pagers, and other mobile devices. This national capability will ensure more people receive Presidential, Imminent Threat, and AMBER alerts. In support of this effort, the first CMAS Forum was recently held. The purpose of the Forum was to convene the alerts and warnings community-including message originators, emergency responder organizations, industry organizations, academia, and organizations representing special needs populations-to address critical issues and determine next steps for the CMAS Research, Development, Test and Evaluation (RDT&E) program. Action teams based around the initiatives that came out of the CMAS Forum were created and are being populated. http://www.cmasforum.com/, contact cmasforum@sra.com.

Commercialization Office is responsible for the development and implementation of a commercialization process and for the execution of two innovative public-private partnerships that leverage research and development efforts in the private sector that are aligned to detailed operational requirements from Department stakeholders. The Commercialization Office also spearheads DHS S&T's outreach efforts that inform the private sector on "How to do business with DHS." See http://www.dhs.gov/xabout/structure/gc_1234194479267.shtm. Contact: SandT_Commercialization@hq.dhs.gov, 1-(202) 254-6749.

Cyber Security Research and Development Center (CSRDC) S&T has the mission to conduct research, development, test and evaluation, and timely transition (RDTE&T) of cyber security capabilities to operational units within DHS, as well as Federal, State, local and critical infrastructure sector operational end-users for homeland security purposes. As part of its cyber security mission, DHS/S&T has established the Cyber Security Research and Development Center (CSRDC). DHS/S&T utilizes CSRDC to focus cyber security RDTE&T efforts and to involve the best practices and personnel from academic private industry and federal and national laboratories. The Cyber Security R&D Center was established by DHS in 2004 to develop security technology for protection of the U.S. cyber infrastructure. For example, the Linking the Oil and Gas Industry to Improve Cyber Security (LOGIIC) project, which addresses security vulnerability issues related to the oil and gas industry's Process Control Systems (PCS) and Supervisory Control and Data Acquisition systems. The comprehensive monitoring system developed in LOGIIC provides an integrated, multi-component security solution that monitors a PCS for abnormal activity. The Center conducts its work through partnerships between government and private industry, the venture capital community, and the research community. This web site provides 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/, contact csrdc@dhs.gov.

Defense Technology Experimental Research (DETER) The DETER testbed was jointly funded by S&T and the National Science Foundation (NSF) and has been open to the research community since March 2004. The centerpiece of the experimental environment is a safe (quarantined), but realistic, network testbed based on a mesh of clusters of homogeneous experimental nodes. DETER is a critical 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. Existing testing facilities cannot handle experiments on a large enough scale to represent today's operational networks or the portion of the Internet that might be involved in a security attack. Industry has only been able to test and validate new security technologies in small- to medium-scale private research laboratories that do not adequately simulate a real networking environment. Newsletters, published papers, videos and update presentations can be viewed at http://www.isi.edu/deter/. Contact testbed-ops@isi.deterlab.net.

Domain Name System Security Extensions (DNSSEC) Deployment Coordinating Initiative To strengthen the domain name system against attacks, S&T has initiated the DNSSEC Deployment Initiative. DNSSEC has been developed to provide 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 web site contains articles, published research papers, DNSSEC Tools, Case Studies, Workshop information and presentation materials. See http://www.dnssec-deployment.org/.

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. See http://www.oasis-open.org to find more information on the EDXL suite of standards and http://www.nimsstep.org to find more information on the NIMS STEP.

FirstResponder.gov's mission is to provide 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. See www.firstresponder.gov.

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

FutureTECH™ program targets critical research/innovation focus areas that detailed the long-term needs of the Department to partner with the private sector, university communities and national labs in the development of technology for future use by Department stakeholders**.** See http://www.dhs.gov/files/programs/gc_1242058794349.shtm. Contact SandT_Commercialization@hq.dhs.gov, (202) 254-6749.

Long Range Broad Agency Announcement (BAA) is a funding mechanism for original research that addresses DHS capability gaps, which are specified in Part I of its announcement under Research Areas of Strategic Interest. It also funds original research that advances the foundations of technical knowledge in the basic sciences. Successful submissions to the Long Range BAA answer questions such as, "What research problem do you propose to solve? How is your solution different from and superior to currently available solutions or from the efforts of others to achieve a similar solution? What data and analysis do you have to support the contention that funding your R&D project will result in a significant increase in capability for DHS?" All of S&T's divisions and special programs receive and evaluate submissions, as appropriate, through the Long Range BAA. For submission instructions, evaluation criteria, and to apply online, visit: https://baa.st.dhs.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. See www.Biometrics.gov, contact info@biometrics.org.

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 standards are focused on developing radios and other components that can interoperate regardless of manufacturer. P25 CAP allows emergency responders to confidently purchase and use P25-compliant products, and the Program represents a critical step toward allowing responders to communicate with their own equipment. In 2009, the first eight laboratories were officially recognized by DHS as part of the P25 CAP. A DHS-approved laboratory is authorized to produce test reports for P25 equipment. NPPD/CS&C/OEC coordinates the implementation of P-25 compliance standards with S&T to promote communications interoperability, and by

encouraging grant recipients to purchase P-25 compliant equipment and technologies with Federal grant funding. See http://www.safecomprogram.gov/SAFECOM/currentprojects/project25cap/, contact P25CAP@dhs.gov.

The Protected Repository for the Defense of Infrastructure against Cyber Threats (PREDICT) will facilitate 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. This initiative represents an important three-way partnership between the federal government, critical information infrastructure providers, and the security development community (both academic and commercial). 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. See https://www.predict.org, contact PREDICT-contact@rti.org.

The R-Tech Newsletter is a monthly feature that discusses technologies of interest to first responders which have received funding, in part, from the Federal government. Interested individuals can subscribe to the newsletter by RSS feed or can download the newsletter at www.firstresponder.gov or www.firstresponder.gov/Pages/Newsletter.aspx.

System Assessment and Validation for Emergency Responders (SAVER) Program was established to assist 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 focuses on answering two questions for the responder community: "What equipment is available?" and "How does it perform?" 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.

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, within resource constraints, to provide long-term science and technology advances for the benefit of homeland security. The focus areas identified by S&T's Research Council, with input from our customers and the research community, summarize the fundamental work needed to support the future protection of our Nation. See http://www.dhs.gov/xabout/structure/gc_1242157296000.shtm. Contact the Director of Research, SandT.Research@dhs.gov , (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 operational requirements documents (ORDs) and a conservative estimate of the potential available market of Department stakeholders**.** See http://www.dhs.gov/files/programs/gc_1211996620526.shtm. Contact sandt_commercialization@hq.dhs.gov, (202) 254-6749.

Support Anti-Terrorism by Fostering Effective Technologies Act (SAFETY Act) is a program managed by the Office of SAFETY Act Implementation (OSAI). The program 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. As part of the *Homeland Security Act of 2002* (Public Law 107-296), 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. See www.SAFETYAct.gov. Contact SAFETYActHelpDesk@dhs.gov, (866) 788-9318.

Technologies for Critical Incident Preparedness (TCIP) Conference and Exposition TCIP highlights DOJ, DHS, and DoD technologies; RDT&E 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. See http://www.tcipexpo.com.

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 meets at least 80% of the operational requirement, in a 12 to 15 month time frame, at a cost commensurate with the proposal. Goals will be accomplished through rapid prototyping or the identification of existing technologies that satisfy identified requirements. See www.firstresponder.gov or www.techsolutions.dhs.gov.

DHS Technology Transfer Program serves as the focal point for technology transfer activities at the Department of Homeland Security. Currently, DHS operates from one centralized Office of Research and Technology Applications (ORTA) to manage technology transfers at each of its laboratories and throughout the Department. The 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 the DHS can have a tremendous potential for commercial applications throughout the nation and dramatically enhance the competitiveness of individual small

businesses as well as expanding areas of exploration and cooperation for all non-federal partners. For more information, visit http://www.dhs.gov/xabout/structure/gc_1264538499667.shtm

Voice over Internet Protocol (VoIP) project researches IP-enabled communication technologies and evaluates promising solutions. This project will enable the emergency response community to confidently deploy and use IP technologies and integrate video, cellular, and satellite communications. In FY 2009, the project initiated testing and evaluation of IP solutions and completed the first VoIP profile as prioritized by the emergency response community. Ultimately, the project will complete the development of a set of standards based on the needs of emergency responders. DHS and the U.S. Department of Commerce (DOC) gathered key stakeholders from both the public safety and industry communities to form a working group. Led by the DHS Office for Interoperability and Compatibility and DOC's Public Safety Communications Research Program, the Public Safety VoIP Working Group works to define and clarify the expectations for VoIP in the public safety environment. See http://www.safecomprogram.gov/SAFECOM/currentprojects/voip/ and http://www.pscr.gov/projects/broadband/voip/voip.php, contact VoIP_Working_Group@sra.com.

Video Quality in Public Safety (VQiPS) As video technology has evolved, the array of options for public safety practitioners has grown and the interoperability challenges have become increasingly complex. Thus the need has emerged for public safety to collectively articulate their video quality needs to the manufacturing community. The 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. See http://www.safecomprogram.gov/SAFECOM/currentprojects/videoquality/videoquality.htm and http://www.pscr.gov/projects/video_quality/video_about.php. Contact VQiPS_Working_Group@sra.com.

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

DHS Centers of Excellence

DHS Center of Excellence: National Center for Risk and Economic Analysis of Terrorism Events (CREATE) develops advanced tools to evaluate the risks, costs, and consequences of terrorism, and guides economically viable investments in countermeasures that will make our Nation safer and more secure. Resources include: **A***RMOR (Assistant for Randomized Monitoring over Routes), IRIS (Intelligent Randomization in International Scheduling), and GUARDS (Game-theoretic Unpredictable and Randomly Deployed Security)***.** GUARDS is a software program that randomizes patrols, inspections, schedules, plans or actions carried out by security agencies. It has been deployed at the Los Angeles International Airport (LAX) for randomized scheduling of LAX police, and for randomizing placement of Federal Air Marshals. It is currently being deployed at the Pittsburgh International Airport and by the Transportation Security Administration at LAX to randomize their security activities. For more information: http://teamcore.usc.edu/security/.

CREATE Internship Placement Program places students in 10-week long summer internships in homeland security-related work. The private sector can benefit from this program by hosting quality interns who are well-versed in homeland security topics and issues and specialize in areas that encourage homeland security solutions.

HS-ANALISER: Homeland Security –Analysis, modeLing, Integrated, Secured Environment and Repository for Decision Support is a software-based system and decision-support tool that allows policy/decision-makers, analysts and researchers to access Homeland Security-based resources and decision-support tools. See http://create.usc.edu/research/50831.pdf.

Executive Program for Counter-Terrorism is a week-long course that is designed to challenge international counter-terrorism leaders and enhance their analysis, coordination, and knowledge of the evolving terrorist threat. See http://create.usc.edu/Executive.

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 will also provide training in the methods of analysis. Short courses designed for police and fire departments aim to help personnel develop safety programs that can be used in the event of terrorism. This is a first-rate aviation safety program based at Los Angeles International Airport. See http://www.viterbi.usc.edu/aviation/.

USC Degree Specializations in Homeland Security Analysis: The University of Southern California has two degree programs with homeland security specializations: Master of Science in Operations Research Engineering (http://mapp.usc.edu/mastersprograms/degreeprograms/ISE/MSORE.html); and Master of Public Policy (http://www.usc.edu/schools/sppd/programs/masters/mpp/).

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

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

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. See http://create.usc.edu/ and http://create.usc.edu/research/Expert Judgment Elicitation Methods.pdf. For more information, contact universityprograms@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.* See http://www.northeastern.edu/alert/ and http://energetics.chm.uri.edu. For more information, contact universityprograms@dhs.gov.

DHS Center of Excellence: Preparedness and Catastrophic Event Response (PACER) optimizes our nation's preparedness in the event of a high-consequence natural or man-made disaster, as well as develops guidelines to best alleviate the effects of such an event. Resources available include a *Modeling & Simulation Catalog, a Model Memorandum of Understanding (MOU) between Hospitals during Declared Emergencies,* and the *Electronic Mass Casualty Assessment and Planning Scenarios Applet (EMCAPS)*. See http://www.pacercenter.org/. For more information, contact universityprograms@dhs.gov.

DHS Center of Excellence: National Center for Food Protection and Defense (NCFPD) defends the safety and security of the food system from pre-farm inputs through consumption by establishing best practices, developing new tools and attracting 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; *Exercise Design and Facilitation; Event and Consequence Models; Continuous Tracking and Analyzing Consumer Confidence in the U.S. Food Supply Chain; Supply Chain Benchmarking Diagnostic Tool; Global Chronology of Incidents of Chemical, Biological, Radioactive and Nuclear Attacks from 1961-2005; Mass Production of Detection and Neutralizing Antibodies; Biosensors Courses; The Biosecurity Research Institute (BRI); The Frontier Program; Food Protection and Food Safety and Defense Graduate Certificate Programs; The National Agricultural Biosecurity Center (NABC); Optimized Detection of Intentional Contamination using Simulation Modeling; Risk Communication, Message Development/Evaluation and Training; decontamination protocols; and Regulatory, Policy, Technical, and Practical Issues related to Contaminated Food Disposal***.** For more information, see http://www.ncfpd.umn.edu/ or contact universityprograms@dhs.gov.

DHS Center of Excellence: National Center for Foreign Animal and Zoonotic Disease Defense (FAZD) protects 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 *Courses on Foreign Animal and Zoonotic Diseases*, *Public and Private sector Awareness Materials, Field Guide to Handling Contaminated Animal and Plant Materials, Mass Livestock Carcass Management workshop, Specialists in Foreign Animal and Zoonotic Diseases, an Avian Influenza Study Curriculum, a Guide to Developing an Animal Issues Emergency Management Plan,* and a compilation of materials pertaining to the *Economic Impact of Foreign Animal Diseases to the United States.* See http://fazd.tamu.edu/. For more information, contact universityprograms@dhs.gov.

DHS Center of Excellence: National Center for Command, Control, and Interoperability (C2I) creates the scientific basis and enduring technologies needed to analyze massive amounts of information from multiple sources to more reliably detect threats to the security of the nation, its infrastructures and to the health and welfare of its populace. These new technologies will also improve the dissemination of both information and related technologies. Co-led by Purdue University and Rutgers University, available educational opportunities are geared towards educating the next generation of homeland security professionals with initiatives that span the entire career development pipeline, ranging from K-12 programs through undergraduate and graduate level work, to professional education and training. For more information, see http://www.purdue.edu/discoverypark/vaccine/ and http://www.ccicada.org/ or contact universityprograms@dhs.gov.

DHS Center of Excellence: Center for Maritime, Island, & Remote/Extreme Environment Security 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, will strengthen maritime domain awareness and safeguard populations and properties unique to U.S. islands, ports, and remote and extreme environments. Programs include the *MARCOOS High Frequency Radar Network* and the *New York /New Jersey Harbor Maritime Awareness System*. See http://cimes.hawaii.edu/ and http://www.stevens.edu/csr/. For more information, contact universityprograms@dhs.gov.

DHS Center of Excellence: National Transportation Security Center of Excellence (NTSCOE) develops new technologies, tools and advanced methods to defend, protect and increase the resilience of the nation's multi-modal transportation infrastructure and education and training base lines for transportation security geared towards transit employees and professionals. Educational programs include *H1N1 Training for transit agency managers and employees, Educational opportunities in transportation* at the Mineta Transportation Institute (MTI), *Online Master of Science in Homeland Security Management degree* from the Homeland Security Management Institute of Long Island University. See http://www.cti.uconn.edu/, http://www.tougaloo.edu/, http://transportation.tsu.edu/NTSCE/home.htm, http://www.policy.rutgers.edu/centers/nti.php,

http://www.southampton.liu.edu/homeland/index.html, http://transweb.sjsu.edu/, and http://www.mackblackwell.org/. For more information, contact 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. Please visit www.start.umd.edu/gtd for more information.

DHS Center of Excellence Global Terrorism Database is an open-source database including information on terrorist events around the world from 1970 through 2007. See www.start.umd.edu/gtd.

Minorities at Risk/Organizational Behavior Dataset is an open-source dataset covering political organizations representing the interests of ethnic groups whose political status and behavior is tracked by the Minorities at Risk project. Currently, the dataset covers 112 organizations representing 22 ethnic groups in 12 countries of the Middle East and North Africa and operating between 1980 and 2004. See http://www.start.umd.edu/start/data/marob/.

Terrorist Organization Profiles is a collection of information that reflects the efforts of the Terrorism Knowledge Base® (TKB®), developed and sponsored by the Memorial Institute for the Prevention of Terrorism (MIPT). Through this project, MIPT collects information on terrorist groups and key leaders of terrorist groups. Through an agreement between START, MIPT, and DHS, START is making TKB® group profile data available to the public through our website. The Terrorist Organization Profiles (TOPs) presents data collected for and by MIPT through March 2008. See www.start.umd.edu/data/tops.

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. Access: Training modules and programs are developed and delivered upon request from a client. 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. See http://www.start.umd.edu/start/ or universityprograms@dhs.gov.

DHS Center of Excellence: National Center for Border Security and Immigration, 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. See http://www.borders.arizona.edu/ and http://www.utep.edu/ . For more information, contact universityprograms@dhs.gov.

The DHS S&T Directorate's *Career Development Grants* (CDG) Program provides competitive awards to support undergraduate and graduate students attending institutions, including the COEs, which have made a commitment to develop HS-STEM curricula and fields of study. These two competitive programs provide educational support, internship, and employment avenues to high quality 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 USCG and the Office of Intelligence and Analysis (I&A).

Minority Serving Institutions (MSIs) Programs in this area include the *Scientific Leadership Award* (SLA) grant program, and the *Summer Research Team* program. Both are intended to 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 COEs. 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.

Scholarship, Fellowships, and Institutional Development Program provides financial support and mentoring to students pursing HS-STEM degrees: the DHS Scholars Program and the Career Development Grants program. The DHS Scholars program competitively awards scholarships to individual science, mathematics, and engineering undergraduate and graduate students.