Statement for the Record

Bradley I. Buswell
Under Secretary (Acting), Science and Technology Directorate
Department of Homeland Security

Before the U.S. House of Representatives
Committee on Appropriations
Subcommittee on Homeland Security

March 26, 2009

INTRODUCTION

Good Morning, Chairman Price, Ranking Member Rogers, and distinguished Members of the Committee. I am honored to appear before you today to update you on the progress of the Department of Homeland Security's (DHS) Science and Technology Directorate (S&T Directorate). I also plan to detail the Directorate's many accomplishments from the past year; discuss current programs on track to provide future technological capabilities to our customers, the operating components of DHS and our Nation's first responders; and describe how our efforts are helping to unify the Department.

I am grateful for the immediate and strong leadership of Secretary Napolitano. She is committed to the mission of the Department: protecting the Nation from terrorist threats and promoting a nation-wide culture of preparedness for dealing with natural disasters. The Secretary has also testified to the importance of greater use of science and technology in improving our capabilities to accomplish that mission. I am pleased to report to you the S&T Directorate has been successful in improving our capabilities across the extremely diverse homeland security mission set.

I am very appreciative of the leadership of the Congress in supporting of the Directorate's endeavors. I am also grateful for the engaged and non-partisan relationship we enjoy. The informed counsel of Committee Members with homeland security oversight, and that of their staffs, has been invaluable to the Department's efforts to position the S&T Directorate for accountability, tangible results, and success – both today and for the future.

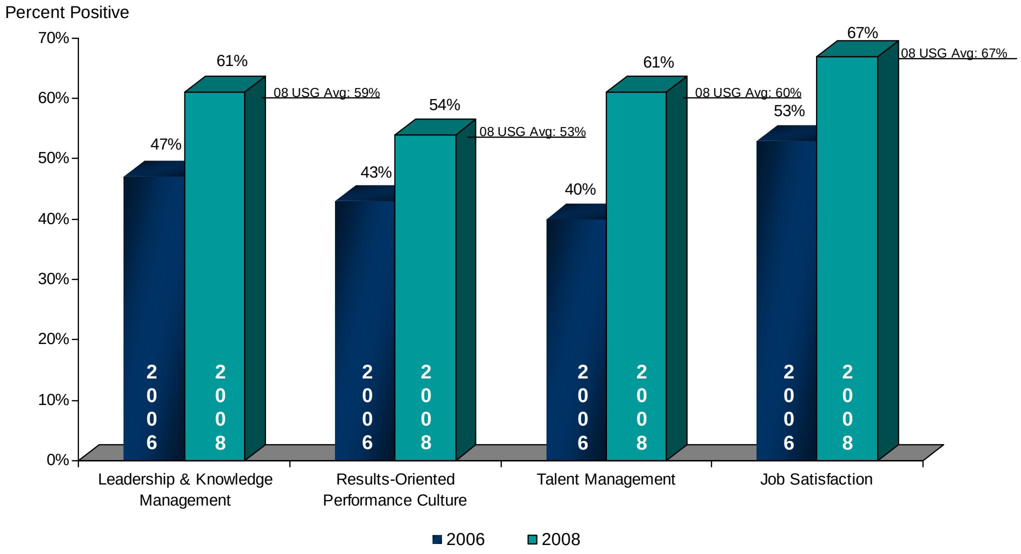
The Committee is familiar with the Directorate's efforts over the past two years to reorganize its structure, research portfolio, and business operations in order to expedite the delivery of cutting edge technological solutions to our customers. I am proud to report that these efforts have been successful, and the Directorate is now fully focused on fulfilling our customers' near-term and long-term technological capability needs. I am obliged to update the Committee on the status of the Directorate's personnel and processes before we focus on the myriad technological achievements we have provided, or will provide, to our customers.

SUCCESSFUL TURNAROUND – PEOPLE & PROCESS

People

I am honored to serve with the many talented scientists and engineers, and other professionals who support these dedicated Americans in our shared mission to field technologies that secure our homeland and defend our freedoms. The Directorate has seen significant improvement in workforce morale over the past two years. This is best highlighted by the results of the 2008 Federal Human Capital Survey which clearly indicate that we are making noteworthy progress on the management shortcomings that previously hindered the Directorate's performance. The 2008 results demonstrate dramatic improvement for the Directorate since the 2006 survey, and indicate that S&T is now on par with the Federal government as a whole.

2008 Federal Human Capital Survey
DHS Science & Technology



While I am pleased with the results of our efforts over the past two years, I am not satisfied. There are still areas that need attention, and I am committed to maintaining the momentum.

Process

Basic Research. The Directorate's basic research portfolio addresses long-term research and development needs in support of DHS mission areas that will provide the nation with an enduring capability in homeland security. This type of focused research investment has the potential to lead to paradigm shifts in the nation's homeland security capabilities through investment in our universities, government laboratories, and the private sector.

During this past year, in order to facilitate better integration and coordination of effort within S&T, the Director of Research established a Research Council and developed the initial draft of the DHS S&T Basic Research Strategic Plan. This plan will outline our strategy for basic research and codify best practices from the members of the Research Council and other stakeholders in the basic research community. To further refine the metrics used in all the Directorate's portfolios, we initiated a contract for the National Academies of Science to study this issue.

Additionally, to better communicate the areas of research in which the Directorate is interested, we issued the initial draft of our basic research focus areas and met with our customers and university and laboratory partners to refine them based not only on what is desirable, but also what is realistically achievable within the realm of cutting edge research. In the coming year we will be distributing the refined version of these basic research focus areas so as to improve communications between S&T and others on our basic research portfolio, thereby encouraging interaction and helping interested stakeholders to provide applicable research efforts.

Innovation. The Directorate's Homeland Security Advanced Research Programs Agency (HSARPA) has implemented a transparent process for identifying, prioritizing, and selecting new High Impact Prototypical Solutions (HIPS) and High Impact Technology Solutions (HITS) projects in the Innovation budget line and has used this process to re-evaluate existing projects and to select future "new start" projects.

The first step is for the HSARPA staff and other members of the Directorate to gather ideas for potential new HIPS and HITS projects from documented needs of DHS customers, solicitations and proposals, discussions with S&T stakeholders, technology conferences and symposia, university, laboratory and industry interaction, and international collaboration. Next, the Director of Innovation/HSARPA screens the list of potential projects to ensure that they meet the fundamental philosophy of the innovation portfolio, namely that though they still contain high risk, they offer substantially higher payoff than programs currently handled in the transition portfolio or an actual acquisition program of record. The Director then presents this list of recommended new start HIPS and HITS to the S&T Corporate Board to ensure the recommended efforts are not redundant with efforts already under way, and to obtain corporate board agreement that the recommended projects are neither more appropriate for the basic research or transition portfolios.

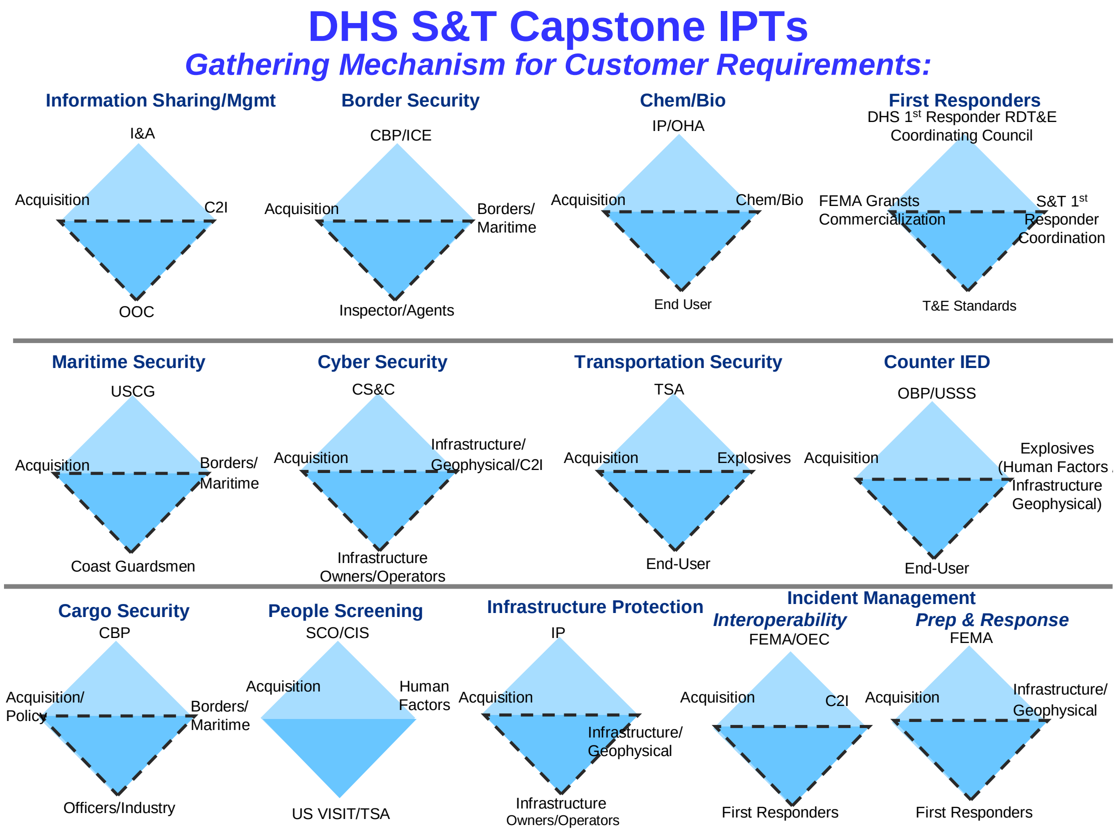
Following concurrence by the S&T Corporate Board, the Director of Innovation/HSARPA presents the list of recommended new starts to the Deputy Under Secretary and the Under Secretary for Science and Technology for concurrence. The final phase of the approval process takes place annually when the Under Secretary presents the recommended new starts to the DHS Technology Oversight Group (TOG) for approval. The TOG is chaired by the DHS Deputy Secretary with membership of the Under Secretary for Management and the Under Secretary for NPPD.

During the past year, HSARPA completed several demonstrations of prototypes that had been developed over the previous two years. Those demonstrations included:

- Future Attributes Screening Technology (FAST)
- Magnetic Visibility (MAGVIZ)
- Resilient Electric Grid (REG)
- Levee Strengthening and Damage Mitigation
- Tunnel Detection
- Biometric Detector
- Resilient Tunnel

The most important process that the Directorate uses is the one that puts us in direct contact with our customers: the Capstone Integrated Product Team (IPT) process. It ensures that we are identifying our customers' highest priority needs and providing near-term capabilities to address them. These Capstone IPTs engage DHS customers, acquisition partners, Directorate Division Heads, and end users as appropriate to align our research, development and product transition activities to their requirements and acquisition activities. The science and technology solutions that are the outcome of this process, referred to as Enabling Homeland Capabilities, draw upon technologies that can be developed and delivered to our customer acquisition programs within three years. As with the Innovation Portfolio, the Under Secretary presents recommended new start programs to the DHS Technology Oversight Group (TOG) for approval.

Our experience over the last year has led us to maintain twelve Capstone IPT areas – Information Sharing/Management; Border Security; Chemical Defense; Biological/Agricultural Defense; Maritime Security; Cyber Security; Transportation Security; Counter IED; Cargo Security; People Screening; Infrastructure Protection; and Incident Management – and add a thirteenth to directly support first responders.


DHS S&T Capstone IPTs

Gathering Mechanism for Customer Requirements:

The thirteenth Capstone IPT was officially announced in February 2009 at the DHS S&T West Coast Stakeholder Conference in Bellevue, Washington.   The conference focused exclusively on First Responder technology needs and existing technological gaps. As an aside, we had a substantial turnout from the First Responder community at Bellevue. The outreach initiative demonstrated at this conference is representative of the larger DHS-wide effort to identify First Responder needs and requirements and bring resources together to address the most pressing issues.

Within the various First Responder communities there are several mechanisms currently employed to research and identify First Responder technical requirements. While the First Responder Capstone IPT will not replace tried and true processes, it will formalize and align those processes to the way the Directorate does business. The First Responder IPT will also allow the community to leverage the processes and relationship the Directorate has developed with the International Community, within the Interagency, and at our Universities.

In order to accomplish this, the IPT will formally establish an Emergency Services Sector Research, Development, Test, and Evaluation (RDT&E) Working Group comprised of representatives from the National Protection Programs Directorate (NPPD), the Office of Infrastructure Protection (OIP), the Emergency Services Sector Coordinating Council (SCC) and the Emergency Service Sector Government Coordinating Council (GCC). This group will serve as the primary engine for identifying technology gaps in the Law Enforcement, Fire, Emergency Management, and Emergency Medical Services areas. Because Federal Advisory Committee Act (FACA) rules apply when communicating RDT&E requirements to the Capstone IPT, a government-only unit comprised of members from the Assistant Secretary for State and Local Law Enforcement, the Office of Health Affairs, the Fire Administrator, and the GCC will officially represent the First Responder community to the IPT.

The Capstone IPT process for First Responders is similar to that of the other twelve IPTs. As technology gaps or technology needs are identified by the RDT&E Working Group, the Directorate will first examine the DHS S&T and FEMA investment portfolio to determine if the requested technology already exists or if R&D is currently underway in the interest area. If a solution is not available or research and development is not underway, the Commercialization Office will communicate the First Responder requirements to the private sector and solicit a solution. The Directorate will also begin the planning necessary to seek a technological solution. The FEMA Grants Office will provide input regarding the availability of grant money to support development and deployment of the requested technology. DHS T&E will play a substantial role in ensuring appropriate rigor is applied to the test and evaluation process and in the use of approved standards.

PRODUCT IS *JOB ONE*

Delivery of technological capabilities to our customers is the reason the S&T Directorate exists. In the past year, the Directorate has had numerous products which we have transitioned to our customers in the Capstone IPT capability areas, and we are on track to continue this performance in the future.

Transportation Security

Air Cargo Screening. In helping TSA meet its congressional deadline to screen 100 percent of air cargo carried on passenger planes by 2010, S&T conducted a number of assessments of Advanced Technology and X-ray machines. Machine and screener performance was evaluated for six different break-bulk systems. Because a majority of air cargo arriving at Independent Air Carriers (IAC) is on wooden pallets, the Directorate also conducted six initial assessments of palletized cargo screening systems. This will relieve IACs from having to break down pallets, screen the individual parcels, and build the pallet back to its original configuration. Over the past year, the Directorate has:

- Completed the congressionally-directed **Air Cargo Explosives Detection Pilot Program** which tested new concepts of operation for screening a significant percentage of air cargo above current levels. Conducted at the San Francisco, Cincinnati and Seattle international airports, the program examined different approaches to screening air cargo for explosives and stowaways. Analytical data, results, analysis and conclusions will be provided to TSA in order to determine how to best use new screening technologies and properly implement new explosives detection technology within the cargo handling systems at major US airports.
- Developed a **mass-spectrometry based trace explosives detection systems** for air cargo screening designed to reduce labor costs and false alarm rates. These systems will be evaluated by S&T and TSA in an operational environment beginning in spring 2009. If successful, these systems will undergo Independent Test & Evaluation against TSA detection standards.
- Developed a **Cargo Screening Metal Detector** to screen pallets of non-metallic air cargo (e.g., flowers, produce). The first prototype system will be delivered for testing by the Transportation Security Laboratory in June 2009. If successful, vendors and shippers can use this technology to screen their products for metal components of Improvised Explosive Devices streamlining the screening process.
- Evaluated the performance of a **modified Explosive Detection Systems (EDS),** originally designed to be used for checked baggage, optimized for screening air cargo for explosives.

Checkpoint Screening. Developed technologies and concepts of operations for TSA to improve checkpoint screening systems throughput, capacity, reliability and effectiveness while minimizing false alarm rates and cost and labor. To support this program's customers, the Directorate:

- Developed a **Digital Imaging and Communications for Security (DICOS)** standard to serve as the standard image file format to enable data exchange between security screening equipment and allow threat detection algorithms to be used in x-ray based screening of checked baggage and carry-on luggage. The draft standard is expected to be released in late FY 2009, and will provide TSA with significant cost savings when acquiring technology by promoting competition among algorithm developers.
- Initiated evaluation of **Magnetic Visibility (MAGVIZ)**, a proof of concept program to identify by chemical name any liquid being carried through a security screening checkpoint. This system was tested at Sunport Airport in Albuquerque, NM, and successfully demonstrated the ability to detect and identify dangerous liquids surrounded by non-hazardous liquids in a 3-1-1 size container tray.
- Conducted **laboratory assessments** to support development of technical requirements for technologies concerned with Whole Body Imaging, Shoe Scanner Systems, and Carry-On Baggage Explosives Detection.
- Completed a prototype **Three-Dimensional Computed Tomography** system for use at checkpoints. These prototypes are down-scaled versions of the systems currently in use at large checked bag screening systems and provide improved explosives detection capabilities. These systems would be especially beneficial in smaller airports where they can serve as "dual use" systems, processing checked and carry on baggage in the same space constrained location. TSA will begin qualification testing for checkpoint use in FY 2009.

Home Made Explosives (HME). As a result of attempted and executed terrorist attacks involving Home Made Explosives (HME), particularly hydrogen peroxide threats, DHS recognized an urgent operational need to detect HME threats to the transportation infrastructure in the U.S. To combat this threat DHS has structured a HME program with the goals of (1) systematically determining the physical and chemical properties of HME threats; (2) identifying, evaluating and improving HME detection and screening methodology; and (3) developing, verifying and validating models to determine HME damage effects. To support this program's customers, the Directorate:

- Sponsored the **development and validation** of predictive modeling tools to predict HME chemistry and potential damage effects caused by HME to be used by the TSA to determine the explosive threat amounts which must be detected in TSA operated environments.
- Tested potential **HME detection technologies and screening methods** through the collection of raw data and images from explosives detection equipment for a wide variety of Commercial Off The Shelf (COTS) EDS, Computed Tomography (CT) and x-ray diffraction equipment to allow TSA to determine the feasible explosive threat amounts which need be detected for various HME explosives threats in TSA operated environments.

Technical evaluations. Evaluated numerous other transportation security technologies for conformity to performance requirements and certification. To support this program's customers, the Directorate:

- Completed conformity assessment of **Advanced Technology (AT) Checkpoint** X-ray equipment. The primary performance requirement evaluated was the Transportation Security Officer ability to identify and detect a wide variety of threats to civil aviation. The evaluation involved development of over 1000 test bags some if which contained functional IEDs with live explosives. The output of this effort drove TSA procurement and deployment of checkpoint AT in FY 2008.
- Completed **laboratory evaluation of three Bottle Liquid Scanner (BLS) devices** and their ability to detect hazardous liquids including liquid explosives. Evaluation included operational usability and suitability requirements along with the capability to distinguish dangerous liquids from those typically carried aboard aircraft. Results from this test will allow TSA to move forward with an operational evaluation of promising products.
- Conducted a series of eight lab assessments of **whole body imagers (WBI)** for use in passenger checkpoint screening. This assessment spanned 18 months involving up to four different imaging devices, 30 mock-passengers and six TSA-certified TSOs per device and per trial to evaluate a subset of TSA-specified detection performance and operational suitability as a pre-condition to TSA piloting and trial deployment at several domestic airports. In addition, these lab assessments that TSL conducted provided data to TSA to enable them to optimize system configuration, training methods and passenger stance protocols.
- Completed Certification Test and Evaluation of the first 600+ bag/hour **High Throughput In-Line Explosives Detection System (EDS).** Successful certification was the culmination of over six months of extensive laboratory testing involving analysis of over 7,000 test objects. Results will permit TSA to install the system in their new Transportation Security Integration Facility in order to evaluate key integration parameters prior to field trials.
- Completed a **multi-year program evaluating two Directed Infrared Countermeasures (DIRCM) systems**, including live-fire tests utilizing real threats and extensive operational

service evaluations on both cargo transport and passenger transport planes, to determine the affectability and suitability of DIRCM technology in the protection the U.S. air transport community against the Man Portable Air Defense System (MANPADS) threat. Final results of this program will be delivered to Congress in late FY 2009.

In the upcoming year, the Directorate will deliver to potential customers, including TSA and mass transit authorities, a rugged canine harness with a suite of sensors to command and communicate with canines off-leash; conduct field tests with TSA canine teams to assess currently available HME canine training aids as viable options for training TSA canines; perform technical evaluations of COTS systems designed for screening palletized cargo; and field test a new Bottled Liquid Screening system with TSA.

Border & Maritime Security

Border& Maritime Security Technologies. The Directorate develops and transitions technical capabilities that enhance U.S. border security without impeding the flow of commerce and travelers by working closely with its operational customers, such as the USCG, CBP, and ICE, to identify gaps in current capabilities and future needs in order to determine and prioritize investments in new technologies for securing U.S. borders. Its area of responsibility encompasses all air, land, and maritime borders, including U.S. ports-of-entry and inland waterways. To support this program's customers, the Directorate:

- Installed a **BorderNet prototype** at the U.S. Border Patrol Station in Douglas, AZ to connect law enforcement officers in the field with real-time tactical information such as detection, sensor data, agent location data, and local geographic features, as well as field access to select law enforcement databases, using a wireless data network and commercial and Government developed software. S&T has an approved Privacy Impact Assessment (PIA) in place for this program (formerly known as BTSNet), which is currently being updated to reflect ongoing project development.
- Installed a prototype system in a **public infrastructure drainage tunnel at** Nogales, AZ, to **detect (illegal) human activities**. The sensor is emplaced behind the concrete tunnel wall to avoid sabotage while reliably detecting the presence of humans. Preliminary testing was completed and successful. Current work is focused on software upgrades for false alarm 'tuning' and improved user interface.
- Developed a distributed, ad-hoc, mesh network capability for **Unattended Ground Sensors (UGS).** This enables the "hopping" of alerts through the network and eliminates the need for every UGS node to be within communication range of a repeater's site. Nodes will "auto-locate" an alternate communication path if one unit fails or is discovered by adversaries. This will enable agents to deploy UGS in many more locations than previously possible.
- Developed and delivered an **immigration model** that serves as a decision-aid tool for border enforcement agencies by determining the tactical implications of changes in immigration/border security policy and operations. This tool is being used by CBP and is being planned for use by the ICE Secure Communities. It can be available to support the Administration and Congress in addressing questions that may arise during future discussions of Immigration Reform.
- Developed an **eco-friendly removal agent for Arundo donax (Carrizo Cane)** along the Rio Grande River to increase border security and officer safety by eliminating possible use of

areas infested with this thickly grown weed as coverage for human and contraband smuggling.

- Deployed two differently designed prototypes of off-shore buoys for an on-going evaluation of **Vessel Detection capability.** This is aimed at improving the Coast Guard's off-shore surveillance capability with detection ranges up to 20 nautical miles from the buoys' locations and at depths up to 4 km, in order to allow sufficient time for the Coast Guard to investigate suspicious vessels before they are in ports.
- Demonstrated the ability to successfully locate an underground tunnel at forty feet with **Tunnel Detection**, a proof of concept project that creates a means to rapidly screen a large geographical area for underground tunnels by using a small unmanned areal platform with a radio frequency transmitter/receiver.

In the upcoming year, the Directorate's Border/Maritime Security projects will include the installation of a North East border testbed to provide a system architecture that supports the integration and evaluation of new sensors and data fusion technologies; the installation of a maritime testbed with the Port of Los Angeles for advanced fusion technologies that will provide DHS Components with an environment to derive changes in Concepts of Operations as a result of new technologies; the start-up of a pilot tripwire system on the Southern border to both sense intrusions and to provide communications to remote locations; a demonstration of a new port and coastal surveillance system in Long Island Sound to evaluate the feasibility of coupling a low cost, off-the-shelf radar with high-end, sophisticated signal processing to detect, track and identify large and small vessels from 0-12 nm in the port and coastal regions; and an assessment of our capabilities to detect and interdict Self Propelled Semi-Submersible vessels. The BorderNet Privacy Impact Assessment is being updated to cover these activities.

Container Security. The objective of the Homeland Security Cargo Security Program is to develop advanced technologies to address supply chain security and to test those technologies for functionality and ultimately for certification as acceptable security devices and/or methodologies. As such, all designs must comply to international standards and trade regulations and be tested in a variety of international supply chain environments in addition to those applicable to the U.S. To support this program's customers, the Directorate:

- Completed the development, prototype delivery (20 from each vendor) of the **Advanced Container Security Device (ACSD)** for testing. The ACSD is a small unit that attaches to the inside of a container to monitor all six sides of the container to report any intrusion or door opening. It will also detect the presence of humans in the container. Vendor is working on correcting certain deficiencies identified by the recent test. Testing is expected to complete by early FY 2010.
- Completed the development, prototype delivery (40 units – 20 from each vendor) and testing of a **Container Security Device (CSD)** prototype which is a small, low cost device, mounted on or within a container, specifically directed at monitoring the opening or removal of the container doors. Vendor is working on correcting certain deficiencies identified by the recent test. Testing is expected to be complete by early FY 2010.
- Developed, delivered and ISO tested a first version of the **Hybrid Composite Container**, which is a potential next-generation ISO shipping container with embedded security sensors. These sensors are designed to detect intrusions from the point of cargo consolidation to the point of deconsolidation in the global maritime supply chain. The container will be

constructed from composite material with embedded sensors. Composites are stronger than steel and hybrid composite containers are expected to be 10-15 percent lighter than current shipping containers. Development and refinement of manufacturing process for hybrid containers are on-going.

- Delivered **Secure Carton** first prototypes for tamper resistance testing (ongoing). These cartons have an embedded tamper-evident sensor and an embedded Radio Frequency ID (RFID) chip which is activated once the carton is sealed and will alert authorities in the event of subsequent tampering or intrusion.
- Completed **Secure Wrap,** a Phase I Small Business Innovative Research Program (SBIR) which is a tamper-indicative wrapping material for palletized cargo. It will enable inspectors to more easily and quickly identify whether the cargo has been tampered. Phase-II development and prototyping began in February 2009.
- Developed software and delivered functional workstations for an **Advanced Screening & Targeting I (ASAT-I)** capability for cargo security. ASAT-I provides next-generation risk assessment and targeting tools to complement the CBP Automated Targeting System (ATS). It provides automated anomaly detection and pattern discovery algorithms to target high-risk cargo. ASAT-II (FY 2009 start) will further advance computer algorithms and software that will automatically collect data from a broad spectrum of sources and combine and analyze shipping information to find suspicious relationships and patterns.

In the upcoming year, the Directorate will continue to mature and transition Cargo Security technologies as described above and initiate a myriad of new projects such as Automatic Target Recognition (ATR)**,** a program to provide automated imagery detection capability for anomalous content (e.g. persons, hidden compartments, contraband) for maritime & air cargo; a SBIR Project to develop a small, highly portable Remotely Operated Vehicle/Autonomous Submerged Vehicle (ROV/ASV) to inspect the interior holding compartments of tanker ships for weapons and contraband; a second SBIR to non-intrusively examine the voids (i.e., fuselage, empennage, wings and fuel tanks, and cargo holds) in General Aviation (GA) aircraft, and the Marine Asset Tracking Tag System (MATTS) to serve as the global communication backbone for the ACSD/CSD and Hybrid composite containers.

Chem/Bio Defense

The Chemical and Biological portfolio works to increase the Nation’s preparedness against chemical and biological threats through improved threat awareness, advanced surveillance and detection, and protective countermeasures. Through its strategic objectives, it seeks to enable comprehensive understand and analyses of biological and chemical threats in the domestic domain; develop pre-event assessment, discovery, and interdiction capabilities for biological and chemical threats; develop capabilities for warning, notification, and timely analysis of biological and chemical attacks; optimize technology and processes for recovery from biological and chemical attack; enhance the capability to identify biological and chemical attack sources; and develop vaccines and diagnostics for high-priority foreign animal diseases (FADs). To support this program’s customers, the Directorate:

- Dedicated the **National Biodefense Analysis and Countermeasures Center (NBACC)**, located in Fort Detrick, Maryland, as part of the National Interagency Biodefense Campus to support law enforcement by characterizing existing biological threats, anticipate future threats, and provide an enduring national forensics capability to support attribution of biocrimes and terrorism. The laboratory is expected to be fully operational by October 2009.

- Delivered the **2008 Bioterrorism Risk Assessment (BTRA)**. The BTRA provides an expansive analysis of bioterrorism risk to help decision makers evaluate risk mitigation strategies. Results are used to prioritize the risks posed by various agents, identify vulnerabilities, and identify associated major scientific knowledge gaps. The report expanded upon the 2006 BTRA to include enhanced threat agents, agricultural (livestock) agents and direct and indirect economic impact.
- Completed the **Chemical Terrorism Risk Assessment (CTRA)**, a first-time assessment of highly toxic chemicals identified through interagency processes as those of potentially greatest concern for homeland security. The assessment developed a quantitative rank order of risk presented by toxic chemical hazards by combining an intelligence informed threat perspective, a science based analyses, and a complex assessment of potential consequences. Completion of this effort informs the acquisition of medical countermeasures, the development and testing of non-medical countermeasures, the development of new procedures to mitigate contamination, and the identification of chemicals on hazard lists developed to improve security in the chemical supply chain to include industrial and transportation concerns.
- Delivered the first **integrated CBRN Terrorism Risk Assessment (iCBRNra)**, a quantitative risk assessment that incorporates intelligence, public health, and scientific information together to inform decision making across the Chemical, Biological, Radiological, and Nuclear threat areas in support of medical countermeasures and other strategic requirements.
- Developed **Consequence Management Guidance for a Wide-Area Biological Attack** to guide decision-makers in remediation of and recovery from a biological incident affecting urban areas. This guidance expands an existing interagency framework to be more operationally useful. It serves as a current baseline and can be used to develop a comprehensive roadmap outlining key science and technology areas as well as planning priorities for a wide-area biological incident.
- Transitioned to the EPA the **Portable High-throughput Integrated Laboratory Identification System (PHILIS)**, a mobile chemical lab system that can be rapidly deployed in the field to support high throughput analysis (several hundred samples per day) of environmental samples that may contain toxic industrial chemicals (TICs) and chemical warfare agents (CWAs).
- Established a formal partnership with USDA for a **Joint Modeling Operational Capability** to provide coordinated response plans to outbreaks of selected foreign animal diseases. The model will support decision making by evaluating the benefits and costs of strategies for mitigating and controlling outbreaks, and will also inform the development of requirements for future countermeasures.
- Received pre-licensing from USDA Center for Veterinary Biologics for the first ever **next-generation molecular vaccine for Foot and Mouth Disease virus** to significantly improve the Nation's ability to prevent, protect and mitigate the effects of an outbreak of FMD. The Foreign Animal Disease vaccines and diagnostics program is on schedule to have the vaccine fully licensed and ready for production by private industry and procurement to the National Veterinary Stockpile by November 2009. Technology used in the next-generation DIVA vaccine will also accelerate the speed at which new vaccines can be produced.

- Established, through interagency consensus, target and near-neighbor strain panels, performance requirements, and validation protocols for the independent evaluation and validation of **assay technologies that detect *Bacillus anthracis***.
- Developed the capability to rapidly and simultaneously **detect four common serotypes of Botulinum Neurotoxin (BoNT)**, a Category A bioterrorism agent. Each of these serotypes can be detected at low levels, which provides the capability to detect trace amounts of the agent. Further testing and validation of the assays in the Laboratory Response Network (LRN) is anticipated in FY 2009.
- Initiated field testing of two major new classes of next generation rapid biological sensors for continuous monitoring of facilities in the **Detect-to-Protect: Triggers and Confirmers Project**. These sensors will detect and identify aerosolized biological warfare agents within 15 minutes, have very low false alarm rates, and be affordable to own and operate by localities. Fieldable prototypes of multiple approaches meeting the Detect-to-Protect requirements are being evaluated in both laboratory and field environments.
- Developed fieldable prototypes (Phase III) of the of the **Autonomous Rapid Facility Chemical Agent Monitor (ARFCAM) and Lightweight Autonomous Chemical Identification System (LACIS)** chemical detectors which employ multiple technological approaches in their systems for chemical threat agent detection applications; one for continuous monitoring of facilities (ARFCAM) and the other for hand-held use by first responders (LACIS). These sensors will address both chemical warfare agents and a broad range of toxic industrial chemical, have very low false alarm rates, and be affordable to own and operate by localities.

In the upcoming year, the Directorate will transition the autonomous biological detector (BAND) prototypes to OHA for testing and possible deployment on large scale to upgrade BioWatch by decreasing time for detection of wide area bioaerosol release; complete guidance for restoration of transit systems following chemical attack; complete development of an integrated response architecture under the Integrated Consortium of Laboratory Networks (ICLN) to improve coordination of Nation's laboratory response networks to large scale CBR attacks; and complete licensure of the first Foot and Mouth Disease vaccine that differentiates between infected and vaccinated animals.

People Screening

The Directorate is developing a variety of technologies and knowledge products that can assist our law enforcement officers in differentiating between law-abiding individuals and those who mean to break our laws or do us harm. As we conduct this research, we are diligent in honoring the rights of Americans. S&T works closely with the DHS Privacy Office and the Office of Civil Rights and Civil Liberties (CRCL) to ensure that our research protects both individual rights and homeland security. Furthermore, we have a robust internal privacy compliance framework in place to ensure that all S&T-funded research that involves or impacts Personally Identifiable Information is reviewed and approved in advance by the Department's Privacy Office. We are also collaborating with CRCL to conduct Civil Liberties Impact Assessments (CLIAs) of S&T research that could impact civil liberties. To support this program's customers, the Directorate:

- Deployed **Mobile biometric collection technologies** with the Coast Guard to identify migrants and smugglers attempting to illegally enter the United States through the waters near Puerto Rico and the Florida Straits. The program has resulted in a total of 3,143 people interdicted at sea, 269 brought ashore for prosecution – with 152 convicted so far. It is estimated that it has reduced the flow of illegal immigration in this area by 60 percent.

- Successfully demonstrated proof-of-concept technologies to acquire **high resolution, high quality single fingerprints without require physical contact**. The success of this effort has resulted in coordination with DoD on future year efforts to develop less intrusive, culturally acceptable fingerprinting technologies. The demonstrated technologies also allows for the possibility to examine three-dimensional features of fingerprints for recognition, providing revolutionary capabilities for fingerprint matching and latent fingerprint examiners in the future.
- Co-sponsored with the National Institute of Standards and Technology (NIST) the creation of the **Multiple Biometrics Grand Challenge (MBGC)** in order to improve face recognition performance. Early results of small data sets show near 100 percent performance when fusing face and iris biometrics together – a critical advancement for biometrics to function in non-contact applications.
- Performed initial validation of **behavioral indicators associated with possession of contraband**, such as weapons, false documents, and illegal drugs. The latest analysis provides statistically significant support that persons demonstrating select behavioral indicators are more likely to possess banned/illegal items. These indicators leverage those used by DHS operational customers such as TSA and CBP.
- Demonstrated proof of concept with TSA's Screening Passengers by Observation Technique (SPOT) program of **MobileSPOT technology**, a hand-held device that will enable the extension of TSA security layers beyond the checkpoint area by enabling SPOT Behavior Detection Officers (BDOs) to wirelessly share information that is currently exchanged manually or not at all.
- Conducted preliminary laboratory validation of **behavioral indicators associated with verbal deception** within a primary or secondary interview environment. These behavioral indicators distinguish deceptive from non-deceptive subjects at a statistically significant accuracy rate and are enabling the development of an automated deception detection prototype and training/training simulation materials.
- Demonstrated **a real-time stand-off system to identify behavioral indicators associated with hostile intent** and deception – the first step in developing a deployed system to detect hostile intent in real time.
- Deployed **deception-detecting techniques and support materials** to TSA and local law enforcement to provide them with behavioral indicators of hostile intent.
- Developed and conducted initial validation of the **Future Attribute Screening Technology (FAST) Theory of Malintent** (the intent to cause harm) for a primary screening environment, identifying specific cues that are diagnostic of malintent.
- Demonstrated **FAST initial sensor integration and command and control framework.**
- Convened the **Community Perceptions of Technology (CPT) Panel** to understand and incorporate community perceptions in the development and deployment of critical technologies within the United States such as microwave vehicle stopping technology, Raman spectroscopy for standoff detection of explosives, mobile biometrics, and acoustic non-linear technology for standoff threat detection.

In the upcoming year, the Directorate will execute malintent detection protocols with over 400 volunteer subjects to test theories and support data analysis; deliver a multi-modal (face, iris, finger) biometrics test and evaluation framework for government-sponsored multi-modal vendor tests that set the stage for incorporation of multi-biometric collection and fusion to support higher throughput screening applications; create a multi-biometric reference research database that will be used to evaluate biometrics algorithms and system performance for use by DHS operational components and continue to improve technical performance through industry and university challenge problems; develop technologies, in coordination with DoD, to collect multiple fingerprints for biometric matching without requiring physical contact; and develop technologies and procedures to enhance screener-performance and reduce human fatigue and injury while reducing training requirements and overall cost.

Cyber Security

The Directorate's Cyber Security program conducts the full spectrum of research, development, testing, evaluation and transition activities related to protecting critical information infrastructure; developing the cyber research infrastructure; and delivering new technologies. These efforts support a broad customer base including critical infrastructure operators/owners in the private sector; the general public; the Federal government; and specific DHS customers such as the US Computer Emergency Readiness Team and the United States Secret Service. To support this program's customers, the Directorate:

- Developed and deployed **Domain Name System Security (DNSSEC)** throughout the U.S. Government to address security weaknesses in the Internet's domain name system (DNS). The DNSSEC standard addresses DNS weaknesses that result in forged or compromised data, DNS cache poisoning, or man-in-the-middle attacks. Development included Federal agencies, private industry, and global Internet owners and operators.
- Funded the **Domain Name System Security (DNSSEC) – Secure Signer** effort to provide certainty for consumers, businesses and government that their web transactions and online communications have not been compromised.
- Funded and distributed **secure Ironkey USB drives** throughout Federal agencies to deliver "always-on" protection against simple and sophisticated cyber attacks – including USB sniffing, physical disassembly, differential power analysis, and chip inspection – to provide secure web browsing, cryptographic authentication, end point security, self-service password recovery, and secure password management, thus resulting in improved security of the data on the drives and a reduction of malicious software-related threats delivered via USB devices.
- Deployed the **Protected Repository for the Defense of Infrastructure against Cyber Threats (PREDICT) – Data Repository** to provide privacy-protected operational network traffic datasets to the cyber security research and development community to help them create and develop new models, technologies, and products which assess cyber threats to the country's computing infrastructure and increase cyber security capabilities.
- Completed the **DHS Secure Wireless Access Prototype (DSWAP)** pilot, a secure wireless access solution that provides enhanced, layered defense beginning with the mobile wireless user, specifically using 802.11 WiFi networks, and extending back to protected networks to minimize risk in using public networks to securely connect to DHS networks. The S&T CIO is working with the DHS CIO to have this accepted as a DHS standard.

- Transitioned **Botnet detection and mitigation technology** to US-Computer Emergency Readiness Team (US-CERT) to provide quicker detection and adaptability in an easily deployable manner against attackers attempting to evade the system.
- Transitioned **Data Visualization Tools** to US-CERT for operational use in a software analysis package for data-monitoring analysis.
- Transitioned to the National Cyber Security Division (NCSD) the **Cyber Scenario Modeling and Reporting Tool (CyberSMART**), an on-line collaborative Exercise Scenario and Modeling Tool to assist cyber exercise developers in identifying where further planning and process improvements are needed. In a pilot project, CyberSMART was used in Mass-Attack, the Massachusetts Commonwealth's first cyber-exercise designed to test communications, operational, and command & control related policies, procedures, and practices. The tool has been transitioned to NCSD and is awaiting a decision on whether to be included in the Homeland Security Exercise and Evaluation Program (HSEEP).
- Delivered to the Internet routing community, both operational and research, **RouteViews,** an enhanced routing data collector that provides scalable, real-time access to Border Gateway Protocol (BGP) data as it is being collected from ISPs around the globe to enable the expansion of internet data sources through the increase of both the number of data collectors and the number of peers monitored (the operational routers from which BGP data is collected). This expanded data will allow faster discovery and more comprehensive analysis of attacks on the Internet routing infrastructure.
- Developed the **Rootkit Detection and Mitigation Technology** to protect against malicious software programs designed to take control of a computer's operating system at the administrator level, where they can often hide from detection by standard anti-malware software. This technology was developed by Komoku, a Maryland company, and acquired by Microsoft in March 2008.
- Developed **Active Malware Protection (AMP)**, a product which provides increased computer security and reliability by capturing malware on the wire as opposed to the traditional technique of capturing it on the host. This technology was developed by Endeavor Systems, a Virginia company, and acquired by McAfee in January 2009.

In the upcoming year, the Directorate will continue the deployment of the DNSSEC solution within the U.S. Government and major domains such as ".org" and ".edu"; (2) initiate the Secure Protocols for the Routing Infrastructure (SPRI) program to enhance the security of the BGP, a major part of the Internet infrastructure; initiate a Cyber Forensics program in partnership with both DHS and external law enforcement participants; and initiate the Homeland Open Security Technology (HOST) program that will promote the development and implementation of open source solutions within US Federal, state and municipal government agencies.

Interoperability

While governance and other human dimensions of communications interoperability are critical to any solution, technology remains at the center of the issue, making research, development, testing, evaluation and piloting of new interoperable technologies vital to the creation of a comprehensive solution. To support this program, the Directorate:

- Launched and operated the Congressionally-required **P25 Compliance Assessment Program (P25 CAP)**. P25 CAP will provide manufacturers with a method for testing their communications equipment for compliance with P25 standards and to ensure it is capable of interoperating across manufacturers. P25 CAP will encourage the inclusion of P25 standards in communications systems while creating a means for the emergency response community to confidently purchase and use P25-compliant products.

- Expanded on the **Radio Over Wireless-Broadband** project, a partnership with industry, local government, NIST, and the Institute for Telecommunication Sciences (ITS) that seeks to bridge existing land mobile radio systems with advanced broadband technologies. Broadband technologies, such as Push-To-Talk over Cellular and the Geographic Information System, allow emergency responders to form talk groups and use location-based services for situational awareness and coordination—ultimately saving critical response time.
- Published **Emergency Data Exchange Language (EDXL) data messaging standards** for numerous programs, including the Common Alerting Protocol (CAP) all-hazard emergency alert system, the Distribution Element flexible message-distribution framework for emergency data sharing, the Hospital Availability Exchange, and Resource Messaging. These information sharing standards will improve emergency preparedness, response, and recovery efforts and will be used partnership with the FEMA Integrated Public Alert and Warning System (IPAWs), to enable local, tribal, and state practitioners to provide reliable and accurate alerts and warnings to more of the public.

In the upcoming year, the Directorate will conduct demonstrations and pilots of the MBR across the Nation; announce the initial group of laboratories that have been assessed as part of P25 CAP and begin testing equipment to ensure that radios from different manufacturers are capable of interoperating; accelerate the development and adoption of voice and data communications standards; and continue to encourage the development and implementation of new, standards-based, non-proprietary solutions that use Project 25, Voice over Internet Protocol, and other voluntary consensus standards.

Information Sharing/ Management

Relevant and timely information is vital for making tactical, strategic, and planning decisions when responding to natural and man-made incidents and disasters. The Directorate provides homeland security practitioners with a toolkit of technologies, processes and mechanisms to support gathering, analyzing, managing, sharing, and protecting information. The current information sharing environment consists of stove-piped communities that have developed their own policies, rules, standards, architectures, and systems to channel information to meet mission requirements. The Information Sharing program works to overcome these barriers by developing national solutions for sharing all-hazards information in manner consistent with national security and legal standards that create new technologies to share, search, and analyze homeland security information across jurisdictional boundaries; provide technologies to enable a distributed, secure, and trusted environment for transforming data into actionable information; and recognize and leverage the vital roles played by state and major urban area information fusion centers. To support this program's customers, the Directorate:

- Deployed the **Critical Infrastructure Inspection Management System (CIIMS),** a new, cost-effective, technology that enables police to more efficiently manage inspections of important structures such as dams, bridges, large industrial complexes, as well as urban areas. CIIMS was piloted in Maryland by the Maryland State Police Department and further developed for the Los Angeles Police Department in an effort called LA Shield to address large urban environments.

- Established and piloted digital image exchange specifications for the **NLETS Image Sharing Program (NISP)** to enable state and local law enforcement personnel to query and retrieve driver's license photos across state lines via the NLETS network. DHS S&T partnered with the National Institute of Justice (NIJ) to examine the technical, policy, and privacy challenges of enabling law enforcement personnel to share interstate driver's license photos for field identification and threat assessment functions. In addition to DHS and NIJ, agencies participating in the interstate photo sharing program include the International Justice and Public Safety Information Sharing Network (NLETS), the American Association of Motor Vehicle Administrators, the North Carolina Highway Patrol, and the South Carolina and Virginia State Police.
- Developed the **Scalable Reasoning System (SRS)**, an advanced web-based and mobile incident analysis and collaboration technology for front-line law enforcement and counter-terrorism personnel. Deployed at the San Diego Automated Regional Justice Information System (ARJIS) and the Port Authority of New York and New Jersey (PANYNJ), SRS provides access to readily usable, up-to-date information analysis tools.
- Developed a **handheld device software application** that retrieves digital photographs from the California Department of Motor Vehicles (DMV) to enable law enforcement personnel away from their office or vehicle to quickly query, retrieve, and view California driver's license photographs on a range of handheld devices (PDAs), greatly enhancing their ability to positively identify individuals in the field. This application was certified by California Department of Justice, and nearly 500 federal, state, and local law enforcement personnel throughout Southern California are currently participating in its operational testing.
- Developed a regional communications architecture **– the State, Regional, and Federal Enterprise Retrieval System (SRFERS) –** to facilitate data sharing and software integration between multi-jurisdictional criminal justice agencies separated by physical and political boundaries. SRFERS uses existing information infrastructures, such as the International Justice and Public Safety Information Sharing Network, the Automated Regional Justice Information Sharing (ARJIS) network and state networks in place to demonstrate connectivity and exchange data in real time across state lines. Through these existing networks, SRFERS provides a toolkit—consisting of successful architectural models, technical specifications for open source messaging applications, transactions and scripts, templates for information sharing agreements, and technical and policy documentation guidance—to enable agencies to seamlessly share justice information.
- Deployed the **Spatial Temporal Visualization (STV) and Criminal Activity Network (CAN)** visualization toolset to the Tucson Police Department. The STV tool enables crime analysts to plot suspicious or criminal incidents near critical infrastructure and explore distribution of those incidents by time period while the CAN visualization tool integrates CBP License Plate Reader data with a local criminal record set to reveal links among subjects who routinely crossed the border and are known offenders in the Tucson region.
- Developed and deployed multiple new data cubes for the **Immigration and Customs Enforcement Pattern Analysis and Information Collection (ICEPIC) System**. These data cubes are intuitive but sophisticated representations of multi-dimensional structured information within the On-Line Analytical Processing (OLAP) database paradigm. This technology is complementary to both relational and graph-based representations, and provides a "third view" of the data supporting summary queries, including trend analysis and statistical analysis.

- Tailored and deployed the **Everest graph visualization and link-analysis tool** to 200 ICE investigators utilizing ICEPIC data sets. This capability provides the ability to create a graph-based view of information from one or more relational databases, and perform graph queries across this view. The ability to ask questions such as, how are two entities connected, what is the shortest path between two entities, and what entities are connected to a known entity, is a powerful complement to traditional relational queries.
- Developed the **Wireless Airport Surveillance Platform (WASP),** an information-sharing pilot program which uses pan-tilt-zoom cameras and an information-sharing network backbone to detect unrecorded and illegal air traffic. During the first phase of the pilot with the San Diego County Police Department in California, WASP identified a significant amount of flight traffic in the San Diego area which was previously unknown to operators. WASP was successfully transitioned to Customs and Border Protection (CBP) in 2008 and is now in the planning phases of deployment with CBP. CBP is planning to expand the use of WASP to several airports and airfields in the southern border area, and then potentially across the Nation.

During the coming year, the Directorate plans to continue with the AZLink, and SRFERS development efforts currently underway along with continuing to deploy CIIMS, NISP, STV CAN visualization toolset and new data cubes for the ICEPIC system. New efforts will be initiated including the piloting of systems analyzing fusion center information usage and sharing; suspicious capability reporting; developing a HSPD-12-related identity management system broadly applicable across the Federal government; and piloting a geospatial analytics tool for use in fusion centers that will support situational awareness and critical decision making.

Infrastructure Protection

The Directorate's Infrastructure Protection portfolio conducts research and development activities based on the 18 Critical Infrastructure/Key Resource (CI/KR) sectors identified in the National Infrastructure Protection Plan (NIPP). This meets the requirements of the Office of Infrastructure Protection (IP) in the National Preparedness and Programs Directorate (NPPD), and requirements set forth in other Homeland Security directives. Some specific program areas include: Modeling, Simulation, and Analysis, Protective Technologies against blast and projectile damage, Response and Recovery Technologies including damage and cascading effects prevention, and finally Advanced Surveillance and Detection. To support this program's customers, the Directorate:

- Transitioned the **Critical Infrastructure Protection Decision Support System (CIPDSS)** to the Office of Infrastructure Protection for inclusion in the suite of operational tools at the National Infrastructure Simulation and Analysis Center (NISAC). The CIPDSS allows analysis of interdependencies among infrastructure sectors and impacts when a sector is struck by an event. It was successfully used in the preparation of the Pandemic Flu study performed by NISAC.
- Conducted test and evaluation of **flexible concrete mats** that could be deployed to protect underwater tunnels by stemming water inflow following a breach. The effectiveness of the mats has led a major U.S. transit system to consider operational deployment of the system.
- Developed new **material solutions to harden tunnels and other mass transit infrastructure** against IED threats. Existing materials, new materials, and innovative combinations are being evaluated for their effectiveness in protecting different types of

tunnels. Results will provide novel solutions and design guidance for transit owners and operators.

- Demonstrated the cover-deployment mechanism for the proof-of-concept **Secure Against Fire and Embers (SAFE)**, a quick-cover application for automatic shielding of a home with a fire retardant tarp to protect against wildfires.
- Demonstrated a **scaled prototype solution for rapidly closing a levee breach using a water-filled tube**. This levee plug was deployed from a floating platform and guided into place where, due to the rushing water, it then conformed to the breach, thereby reducing the flow of water by approximately 95 percent.
- Demonstrated the **Resilient Tunnel** project, an early prototype of an inflatable tunnel plug to protect tunnels from fire, flooding, and potentially other hazards. Continued development of inflatable plugs is being done in close coordination with the Washington, DC Metro and the Port Authority of New York and New Jersey in order to provide a cost-effective solution for isolating hazards in transit tunnels to protect occupants and system infrastructure.
- Demonstrated across a three meter cable the proof of concept **Resilient Electric Grid (REG)**, a project which incorporates high temperature superconducting technology to ensure the reliable distribution and protection of electrical power acting as a fault current limiter for both DC and AC power to prevent rolling brown outs and black outs.
- Demonstrated a **prototype wireless security system** to monitor and assure the delivery of milk, milk samples, and security information from dairy farms to the dairy plants. Potential exists for broad use across the dairy industry. Having been successfully tested through some 50 loads from dairy farm to commercial plants, this technology will be commercial ready in December 2009.

In the upcoming year, the Directorate will conduct an analysis of existing surveillance technologies and select sets of sensor systems (optical, infrared, ultraviolet, and acoustic) appropriate for monitoring selected infrastructure types; begin development of computational models for blast effects on tunnels, bridges, and urban environments, and conduct experiments to validate the numerical predictions; and focus response and recovery technologies on rail cars carrying chlorine, a toxic inhalation hazard (TIH) material and design and demonstrate a recovery transformer in a laboratory environment.

Preparedness and Response

In the event of a terrorist attack, natural disaster or other large-scale emergency, the Department is responsible for providing a coordinated, comprehensive federal response so as to mount a swift and effective recovery effort. The Preparedness and Response program focuses on the Directorate's effort for ensuring that emergency response professionals are prepared for any situation. To support this program's customers, the Directorate:

- Coordinated national capabilities in atmospheric modeling and provided Federal prediction of atmospheric hazards and their consequences with t**he Interagency Modeling and Atmospheric Assessment Center (IMAAC).** In the past year, IMAAC responded to over 1000 requests throughout the United States, including several fires and chemical releases such as a downwind smoke plume from fire caused by an accidental plane crash into an apartment building in New York, NY, multiple explosions and fire at the Barton Solvents chemical plant in Wichita, KS, chlorine release at a water treatment facility in Berthoud, CO, and the derailment of five phosphoric railcars in Chicago, IL.

- Demonstrated **Man Portable Interoperable Tactical Operations Center**, a services-oriented portable platform that can be transported to an incident scene in an SUV, truck, boat, helicopter or trailer. MITOC is an integrated suite of commercial-off-the-shelf (COTS) tools to enhance communications, situational awareness, radio/voice/data interoperability and applications access developed in support of the Kentucky Critical Infrastructure Protection Program (KCI).
- Field tested a **concealable escape hood** for Secret Service agents which provides fifteen minutes of protection agent chem/bio attacks.
- Developed early concepts in support of **Physiological Health Assessment Sensor for Emergency Responders (PHASER)**, a program for monitoring the vital measurements of agents in real time through the use of intelligent algorithms, in order to provide an alarm to both responder and commander if a responder is going to experience any health threatening events.
- Tested the **Geospatial Location Accountability and Navigation System for Emergency Responders (GLANSER)** to allow for tracking of first responders inside buildings, below ground, above ground, and in rubble where GPS is denied, with an accuracy of three meters in all dimensions.
- Developed and tested the **Controlled Impact Rescue Tool (CIRT)** for Urban Search and Rescue teams to breach concrete barriers in a safe and efficient manner.
- Developed the **Unified Incident Command and Decision Support (UICDS)** Information Architecture, a blueprint for managing and sharing incident information across state and local jurisdictional lines and with DHS and other federal agencies. This national architecture, a response to issues identified in the 9/11 Commission Report, is aimed at establishing a set of standards to which solution developers for incident management tools will adhere in order to ensure that recipients of DHS funds at the state/local level will procure incident information management systems that comply with the UICDS standards in order to solve the information interoperability problems. While the initial framework was completed in 2007, the architecture is currently being developed and will be tested in FY 2009.
- Demonstrated **Training, Exercise, and Lessons Learned (TELL)** a prototype system to enable cost effective training for emergency management teams. Using models and simulations and leveraging graphics engines from the gaming industry, the system provides for a live, virtual, and constructive environment so policy makers, elected officials and incident commanders can quickly assess the consequence of their decisions during an incident. The TELL prototype was used in preparation for exercises in Anaheim, California and Cincinnati, Ohio and will be deployed at the FEMA National Exercise and Simulation Center (NESC) for nationwide exercises and operations analysis. This capability is being developed in response to the Katrina White House Lessons Learned Report.

In the upcoming year, the Directorate will deliver a report detailing temporal and geospatial analysis of needs for shelter, food, and disaster relief as identified by callers into the Texas 2-1-1 System during Hurricanes Katrina and Rita in order to provide first responders/response planners with the ability to more accurately plan for resource requirements and evacuation strategies in future catastrophic events; test the UICDS system; demonstrate a concept prototype of PHASER to validate system requirements, architecture, and concept of operations; utilize TELL to conduct disaster planning training scenarios to prepare FEMA decision and policy makers to validate their plans, procedures, tactics, and doctrine when responding to major events; test and validate GLANSER against a prioritized list of technology challenges (i.e., underground, over ground) at major urban areas such as New York City and Seattle; seek NIOSH certification for the concealable hood so that it can become available as a commercial product; and deliver the iEOC connectivity solution deployed in Seattle to the Cincinnati urban area to enhance situational awareness during an emergency incident.

Counter Improvised Explosive Devices (IED)

The Directorate established the Program Executive Office for Countering Improvised Explosive Devices (PEO (C-IED)) to manage counter-IED efforts in response to the direction provided by Homeland Security Presidential Directive 19 (HSPD-19), *Combating Terrorist Use of Explosives in the United States*. PEO-(CIED) focuses its portfolio in following areas: Prevent/Deter, Predict, Detect, Defeat, and Respond/Mitigate. To support this program's customers, the Directorate:

- Developed the **Standoff Technology Integration Demonstration Program (STIDP)** to provide for the evaluation of a layered approach to security against IEDs. It involves the integration of sensors and technologies into a unified system to detect the approach of a person carrying an IED. The system was successfully tested in Kennewick, WA, in October-November 2008. The data collected will be very valuable in highlighting the outstanding challenges in screening crowds of people at large public events, and in demonstrating how multiple systems can be integrated into a comprehensive approach to screening that will be minimally intrusive and will provide warning of IEDs early enough for action to be taken to prevent the IED from being used as intended.
- Developed an **X-Ray Backscatter System** to detect, diagnose, and defeat vehicle-borne IEDs (VBIEDs). This system provides bomb technicians with the capability to examine suspect vehicles when access to only one side is possible. It has been delivered to a company to integrate into a robot, and the integrated system will be demonstrated in 2009 when it will then be further evaluated by a select bomb squad.
- Characterized **VBIED disruption tools** for validation and testing against mock vehicle bombs as part of an operational database for use by Bomb Squads.
- Developed a **real-time, 360-degree, imaging system** for the detection of concealed objects on people which does not require an individual to stop and "pose" while being interrogated.
- Tested the decommissioned **Waldo Hancock Bridge** to understand the vulnerability of vintage bridge components to terrorist attack scenarios and gain data to enable improvement of numerical models to predict bridge cable response to an IED attack.

In the upcoming year, the Directorate will demonstrate a new VBIED disruptor and make it available for Bomb Squad evaluation and publish reports on trends in support for jihadi terrorism within the United States based on the results of existing surveys; characteristics of groups that use IEDs and trends in IED use over time based on analyses of quantitative databases; and de-radicalization initiatives in five countries and their applicability to the U.S. context.

First Responder Technologies

Although our thirteenth IPT is new and will serve to better coordinate our support of the first responder community, many of the technologies that Directorate has delivered to operational components of DHS will also help first responders. To support this program's customers, the Directorate:

- Developed the **Digital Ink Library** for the Secret Service forensic investigators to create a quick-reference database of inks critical to the investigation of criminal and terrorist casework involving fraudulent financial documents (such as checks and money orders), property and asset documents.
- Demonstrated a prototype **Handheld LED-Based Incapacitator (Dazzler)** to serve as a less-than-lethal technology to better control hostile persons in a standoff environment.
- Facilitated the technology transfer of the U.S. Air Force's **ROVER air to ground surveillance system** program making it available to requesting state and local first responders to assist with firefighting and law enforcement activities.
- Produced **publications for First Responder groups** by the Environmental Measurements Laboratory (EML). Publications include Urban Atmospheric Plume Models for Emergency Response; Dosimeters; and Technologies for Radioactive Decontamination of Building Surfaces.
- Developed **prototype protective suits** using nanotechnology materials and multiple layers to provide active protection elements to block hazardous chemical/biological agents. The suits, several of which have been produced, also have fire retardant properties and are undergoing detailed testing this year.

The Directorate's First Responder Technologies (R-Tech) Division is another avenue by which we deliver products to the First Responder community. Comprised of the Tech Solutions and Tech Clearinghouse subdivisions, R-Tech uses interaction and information sharing with First Responders to provide quick-reaction S&T solutions to their capability gaps. To support this program, the Directorate:

- Produced the **FireGround Compass** to provide Firefighters with a ruggedized portable tool that enables them to maintain their reference point as they fight interior structural fires.
- Prototyped an **Ocular Scanner** to provide the emergency medical service (EMS) community a rapid screening technology for victims with possible exposure to a wide variety of hazardous and toxic agents.

Within the next year, the R-Tech intends to transition a Next Generation Self Contained Breathing Apparatus and Three-Dimension Locator System to Fire Fighters.

Additionally, some core S&T investment has been directed at first responder needs. To support the First Responders over the past year, the Directorate has:

- Developed a pilot program for a **Digital Multi-Band Radio (MBR)** to allow communications interoperability across multiple bands without a gateway or other bridging technology during emergency situations. S&T completed privacy compliance documentation for this pilot project.
- Developed the **AZLink wireless technology system** under the Regional Information Sharing and Collaboration program which provides law enforcement officers with the capability to use PDAs to access information—including criminal histories, mug shots, driver's license data, maps aerial photographs, and incident reports—that they otherwise would need a computer system to access.
- Established the **RealEyes** system to allow users to send and receive live video and geospatial coordinates, view video from fixed or mobile cameras and receive data from a field

command post using basic cellular technology in order to increase situational awareness for law enforcement operations and emergency situations. S&T has completed a PIA for this project.

In February 2009, S&T assumed from FEMA **responsibility for the System Assessment and Validation for Emergency Responders (SAVER) Program** to assist emergency responders making procurement decisions. SAVER conducts objective assessments and validations on commercial responder equipment and systems and provides those results along with other relevant equipment information to the emergency response community in an operationally useful form.

UNIFYING DHS

S&T, by virtue of our role supporting operating components across the Department, is in a unique position to help accelerate the maturation and unification of the Department. To be sure, the Capstone IPT process has helped do that. Additionally, S&T provides other Department-wide services that help DHS operate better as one Department.

Test & Evaluation

Section 302 (12) of the Homeland Security Act of 2002 (PL 107-296) assigns me the responsibility of "coordinating and integrating all research, development, demonstration, testing, and evaluation activities of the Department." The S&T Directorate established the Test and Evaluation and Standards Division (TSD) in FY 2007 to develop Department-wide T&E policy and provide T&E oversight of the major acquisition programs. TSD is working closely with DHS Undersecretary for Management and all DHS components to develop and implement a robust department-wide Test and Evaluation (T&E) policy that will be fully integrated into the Department's Acquisition process framework. The Directorate/TSD has created a draft T&E Directive that complements the new DHS Acquisition Directive (Management Directive 102-01). Together these policies will provide the appropriate component review and DHS oversight for test planning, execution and reporting. The T&E policy will require components to participate in development and approval of the Test and Evaluation Master Plan (TEMP) that will describe the necessary Developmental Test and Evaluation (DT&E) and Operational Test and Evaluation (OT&E) that must be conducted in order to determine system technical performance and operational effectiveness and suitability throughout the development process. TSD is currently providing oversight to major acquisition programs by participating in T&E working groups, approving TEMPs, approving Operational Test Plans, participating in Operational Test Readiness Reviews, observing testing, and participating in Acquisition Review Boards. Over the past year, we have:

- Established a **T&E Council** to advise the senior DHS management in matters relating to T&E. This Council includes participation by all components in promoting T&E best practices and lessons learned, ensuring adequate T&E infrastructure, and establishing consistent T&E policy and processes for use in acquisition programs throughout the Department.
- Provided **T&E oversight** on critical acquisition programs throughout the Department, including Advanced Spectroscopic Portal (Cargo) ASP(C), BioWatch Generation 3, Secure Border Initiative network (SBInet), Air/Sea Exit, National Cyber Security Program (NCSP),

U.S. Visit, Western Hemisphere Traveler Initiative (WHTI), Secure Flight, Transformation and Systems Consolidation (TASC), USCIS Transformation, Transportation Worker Identification Card (TWIC), and Automated Commercial Environment (ACE).

- Partnered with the United States Navy (USN), NIST and DOJ to develop an **initial set of standard test methodologies** applicable to small unmanned aerial systems (sUAS) in support of law enforcement and urban search and rescue missions.

Standards

S&T is the Standards Executive for the Department, with responsibility for coordination of standards activities for the entire DHS as prescribed in OMB Circular A119 and the National Technology Transfer and Advancement Act (PL 104 -113). Standards for the DHS components include performance specifications, documentary standards, measurement standards and process standards as well as interoperability and safety standards. The Office of Standards within TSD has three main functions: 1) coordination of standards within the Department, 2) outreach to the private sector standards development community, and 3) management of a program to develop critical standards for homeland security applications. The Office manages the processes for formal adoption of standards as *DHS National Standards*. The Office also coordinates with private sector Standards Development Organizations (SDOs) that address the homeland security community, ensuring that the standards produced meet the requirements of the DHS components as well as state, local and tribal users of equipment and processes. The Office also manages an investment of funds in development of standards to meet mission needs. This includes evaluating standards needs; participation in standards development planning; coordinating standards development efforts with DHS components and other state and federal agencies and appropriate SDOs; and supporting activities at NIST, NIOSH, DOD and the national labs and other partners in standards related technology development. Over the last year, we have:

- Established an **intra-agency accreditation and certification program** with FEMA, the DHS Private Sector Office, the DHS OIP, and the DHS Office of General Counsel (OGC) to help ensure emergency preparedness and business continuity in the private sector.
- Developed a **Standards Council** to support the department-wide development and adoption of standards. In the last year, the Council has adopted twenty-one new standards for homeland security mission needs, including the American National Standard for High-Visibility Safety Apparel, the Headwear American National Standard for Industrial Head Protection, the Common Alerting Protocol v1.1, the NIOSH Statement of Standard for Chemical, Biological, Radiological, and Nuclear (CBRN) Powered Air-Purifying Respirators (PAPR), the Emergency Data Exchange Language (EDXL) Distribution Element, v 1.0; and sixteen additional National Fire Protection Association Standards.

Federally Funded Research & Development Centers (FFRDCs)

The Directorate recently established two new FFRDCs, the Homeland Security Studies and Analysis Institute (HSSAI) and the Homeland Security Systems Engineering and Development Institute (HSSEDI), which it will manage on behalf of the Department. These institutes will promote fair and open competition for the development and delivery of Department capabilities by providing independent and objective technical expertise. HSSAI will provide special technical expertise to Department mission owners to help them transform mission-level goals into strategies, operational requirements, and performance metrics constrained by cost and schedule. The HSSEDI will provide expertise in support of the Department's acquisition process by assisting in the development of technical concepts, standardized technical data packages, development modeling and simulation, and developmental testing and lab experiments. Through their long-term relationships with the Department, I believe these new FFRDCs will contribute substantially to reducing our Nation's risk to terrorism and catastrophic incidents.

<u>Commercialization and Private Sector Engagement</u>

The Directorate's Commercialization Office and the Office of SAFETY Act Implementation (OSAI) have both contributed to expand upon and improve the Directorate's relationship with business and industry. Responsible for creating initiatives that identify, evaluate and commercialize technology for the specific goal of rapidly developing and deploying products and services that meet the specific operational requirements of our customers, the Commercialization Office establishes and fosters working relationships with the private sector to facilitate cost-effective and efficient product/service development efforts.

In the past year, OSAI has been responsible for coordinating 179 applications from industry partners seeking Federal protection for their technology under the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act). This office links the private sector with not only DHS S&T, but also other members of the Federal government

The Directorate also officially stood up the Commercialization Office in 2008 to develop and execute programs and processes that identify, evaluate and commercialize widely-distributed products or services that meet the operational requirements of the Department of Homeland Security's operating components, first responder community, critical infrastructure/key resources owners and operators and other Department users. It is committed to conducting outreach with the private sector in order to engage and leverage the expertise, skills and resources of the private sector. This outreach includes a concerted effort to engage small, minority, disadvantaged and HUB Zone groups. As a result of these efforts, the Commercialization Office has compiled a listing of well-over 300 companies, outlining over 2,000 technologies, products and/or services that may possess potential alignment to DHS needs. Information has also been compiled to show the number of small, medium and large businesses with whom the Commercialization Office has interfaced. A majority of those companies are small businesses.

Since its inception, the Office has published a number of materials, including briefs, books and articles that outline the major activities of the Commercialization Office and provide readers with easy-to-understand guides to execute effective detailed operational requirements documents (ORDs) and the newly created and implemented commercialization process. Furthermore, the Office has published three popular books to assist in the development of detailed operational requirements. These books serve as a useful resource to explain both the critical role of detailed requirements to cost-effective and efficient product development, and also as an easy-to-use guide to aid in the articulation of requirements.

Another avenue by which the Office performs outreach to the private sector is the System Efficacy through Commercialization, Utilization, Relevance and Evaluation (SECURE) Program, an innovative public-private partnership in which DHS leverages the skills, expertise, and resources of industry to develop products or services aligned to DHS-written and vetted ORDs. Here, DHS posts detailed ORDs on its web portal (http://www.dhs.gov/xres/programs/gc_1211996620526.shtm), along with a conservative estimate of the potential available market (PAM) of a given product/service and invites the private sector to use this information to formulate a business case to pursue potential sales opportunities found within DHS operating components and its many ancillary markets including first responders and CI/KR owners and operators. This program has been well received by the private sector who has been asking DHS to provide more information into the detailed needs and requirements of its stakeholders.

CONCLUSION

I am glad to report that, with our People and Processes securely in place, the Department of Homeland Security Science and Technology Directorate has made significant progress this past year in getting product to our customers. Doing so has helped enable DHS to better protect our Nation. I look forward to working with the Committee to ensure continued success in both the near and long-term future.

Members of the Committee, I thank you for the opportunity to meet with you today and look forward to answering your questions.