Statement for the Record

Dr. Charles E. McQueary
Under Secretary for Science and Technology
Department of Homeland Security

Before the U.S. House of Representatives
Committee on Science

February 15, 2006

INTRODUCTION

Good morning Chairman Boehlert, Congressman Gordon, and distinguished members of the committee. It is a pleasure to be with you today to discuss the research and development activities of the Department of Homeland Security's (DHS) Science and Technology (S&T) Directorate.

As this committee and many of our Nation's leaders recognize, advancements in science and technology play a vital role in protecting our Nation from natural and man-made disasters. Making such advancements happen – carrying them from their hypothetical beginnings to real-life applications – is the job of the S&T Directorate.

We are committed to developing cutting-edge tools and systems that will enable the dedicated men and women who protect and secure our homeland to serve more effectively and efficiently. Providing these end-users at all levels of government with the technological capabilities they need, regardless of the type of threat, is our most important mission.

For example, in the days and weeks that followed Katrina, S&T Directorate staff provided valuable subject matter expertise in diverse areas, including emergency responder communications, evacuation logistics, robot-assisted search and rescue, appropriate technology applications, hazardous biological materials disposal, and site preparation, and rapid deployment of mobile and modular shelters. Our staff also contributed modeling and simulation analysis in areas that include petroleum shortages, disease impacts, critical infrastructure damage, and economic impact. In addition, a number of staff members worked as volunteers, supporting Federal Emergency Management Agency (FEMA) in the relief effort.

Many of our ongoing efforts are improving tools and systems that will enhance emergency response capabilities. We are developing standards for emergency response to ensure the reliability of equipment and processes; developing personal protective equipment for emergency responders when operating in hazardous chemical, biological or nuclear environments; and developing interoperable systems to keep the lines of communication open and clear during a disaster. In addition, the S&T Directorate made significant organizational strides:

- With the transfer of the Transportation Security Laboratory into the S&T Directorate, we completed the plan to consolidate existing research, development, testing and evaluation (RDT&E) within DHS. Given our principal responsibility of coordinating and organizing research and development (R&D) activities throughout the Department, I consider this a major accomplishment that will enable the Department to maximize its science and technology resources.
- The S&T Directorate also made internal management changes that will enable us to productively focus our efforts and work more efficiently. Last year, we established the position of the Chief Financial Officer to oversee finance, budget, planning, and program analysis and evaluation. We also established the

position of Director of Plans, Programs and Requirements to coordinate the direction and activities of the S&T Portfolios. I will describe these Portfolios further when I discuss the organization of the S&T Directorate.

- As a three-year-old organization, I am very proud of the great progress the S&T Directorate has made on creating a Strategic Plan that will solidify our five to ten-year-vision for RDT&E. An accompanying performance management system now in development will enable us to establish highly effective, adaptable business operating policies and procedures that will position the organization to meet the current and future needs of our Nation, regardless of the threats we face.

SHORT AND LONG-TERM RESEARCH

At the S&T Directorate, we know we must also push qualified technologies out of the development pipeline faster and deploy them in actual operating environments so that we are better prepared the next time we are put to the test. To that end, the Directorate has focused its efforts on near-term development and deployment of technologies. However, as part of the Nation's science and technology complex, we recognize the importance of a sustained effort to expand our knowledge and resource base for the future.

Our investments are diversified not only in terms of challenges and opportunities, but also in terms of technological maturity as well. Some scientific problems are basic — we must achieve a core understanding of some phenomena. Others are problems of application — we must learn how to apply our knowledge and understanding of an issue or problem to our own mission. Finally, other technological problems involve engineering development — we must investigate and determine how to move applied knowledge from the laboratory bench to the user. The Department invests in all three. We conduct and sponsor *basic* and *applied* research as well as *advanced technology development*.

- Basic research is sponsored in the expectation that its results will eventually give us new and better ways of accomplishing our mission. For example, understanding terrorist motivations and being able to predict intent; or improving our fundamental knowledge of the properties of non-traditional chemical agents.
- Applied research takes what we already know how to do, and forms it into a useful homeland security application. Integration of biometric data into identification documents and devices used to secure shipping containers during transit are examples of this type of activity.
- Advanced technology development leads to the invention of new devices and systems that can ultimately be transitioned to end users. Our new handheld scanners for chemical countermeasures are a good example of this.

These three kinds of work have very different timetables. Basic research has the longest — it may take a decade or more before a fundamental discovery results in a technology deployed in the field. Applied research tends to progress in months and years. Developmental research is closest to the user — here we work to take advantage of identified opportunities to rapidly develop technologies and deliver them to end users.

In fiscal year (FY) 2005 approximately 2 percent of our funding went to basic research, 79 percent to applied research, and 19 percent to developmental research —very similar to our FY 2004 funding distributions. I expect the distribution in FY 2006 and FY 2007 to be similar. In addition, it is important to note that the S&T Directorate has established an improved method for tracking these types of obligations, which will improve the accuracy of these estimates in the future.

FY 2005 ACCOMPLISHMENTS

I am pleased to report to you the progress we have made in just three years. Much of the work the S&T Directorate carries out requires years of scientific pursuit before it comes to fruition. However, we are beginning to see knowledge and technology emerge that will provide the foundation for strong and resilient homeland security for the Nation.

I would like to highlight in more detail the accomplishments in our research and development programs over the past year.

Regarding our efforts to develop and implement chemical, biological, and explosive countermeasures, we:

- Initiated deployment of BioWatch Enhancement (Generation 2) in more than 30 U.S. urban areas, in collaboration with local partners This enhancement places significantly more air collectors in the top threat cities (including collectors that cover transit systems and special events), allowing them to further increase their broad population protection while also providing targeted coverage of their most vulnerable venues.
- Conducted detailed technical material threat assessments on six agents. This work is done in direct support for the procurement of countermeasures under the DHS/HHS BioShield program.
- Began operating the National Bioforensics Analysis Center (NBFAC) as the Nation's lead facility for technical analysis of forensic samples in order to support attribution, or identify perpetrators, of biological attacks.
- Approved a record of decision on the Environmental Impact Statement (EIS), awarded an architect-engineer design contract, and awarded a contract for construction management services for the National Biodefense Analysis and Countermeasures Center (NBACC).

- Completed and provided the FY 2006 Bioterrorism Risk Analysis to the Administration. This risk assessment, mandated by Homeland Security Presidential Directive (HSPD)-10, is targeted to inform national plans and priorities for biodefense investments and will be a helpful tool to guide DHS policymakers regarding the Department's efforts to anticipate, prevent and respond to acts of bioterrorism.
- Conducted an Interagency exercise to study an incident involving persistent highly toxic chemical agent release.
- Transitioned the Program for Response Options and Technology Enhancements for Chemical Terrorism (PROTECT) networked chemical detection system to the New York City Metro Transit Authority. PROTECT is a chemical detection and response system that was designed for public facilities. It was first installed in the Washington, D.C. metro transit system, and is now operating in the New York and Boston subway systems as well.
- Began establishing the Explosives Knowledge Center, which will enable State, local, and tribal communities to assess the risks of explosive attack and the costs of countermeasures.
- Drafted the first-ever performance standard for a point chemical agent vapor detector for use by civilian responders which is being vetted through the standards organization, ASTM International.
- Developed standards for calibration and optimization of performance for hand-held, trace-explosive detectors.

Within the areas of support to the Department's components, we:

- Conducted an exercise with Customs and Border Protection (CBP) under the Northern Border Security Initiative that identified capability gaps and the technologies needed to address them. The exercise identified what technologies both Canada and the United States agree will improve border security capabilities. The S&T Directorate will use these outcomes to help focus and maximize the development of border security technologies. A report to Congress was delivered in January 2006 on this issue. This effort was in support of CBP.
- Conducted end-to-end testing of the Border and Transportation Security Network (BTSNet) wireless communications backbone installed at the U.S. Border Patrol Station in Douglas, Arizona. The testing focused on the transfer of data from handheld and vehicle-mounted mobile computers to the border patrol station via an existing tower infrastructure. This effort was in support of CBP.
- Designed, built, and tested through the Maritime Automated Scene Understanding (ASU) project, a system that fuses RADAR, camera, and Automatic Identification System (AIS) data, and alerts watchstanders to

anomalies in the coastal environment. This effort was in support of the U.S. Coast Guard.

- Completed Phase I design of the Advanced Container Security Device (ACSD). The ACSD is a security device being designed to monitor and communicate security breaches from each of the six sides of a container, as well as detect human presence inside containers. This effort was in support of CBP.
- Developed the Supply Chain Security Architecture (SCSA) that gives DHS the capability to bridge data and information between container security devices and the National Targeting Center. This effort was in support of CBP.
- Brought the Interagency Modeling and Atmospheric Analysis Center (IMAAC) to full operational capability. IMAAC integrates the Nation's best modeling capabilities to provide accurate information to predict the movement and spread of the contaminate cloud in the event of a major disaster or terrorist attack, thereby saving lives and assisting with timely response decisions. This effort is in support of Federal, State, and local response organizations through the Homeland Security Operations Center (HSOC), serving as the dissemination point for the Department.
- Established the "Training Exercise and Lessons Learned" program to support continuous improvement of our Nation's preparedness to respond to catastrophic events, as called for in HSPD-8, "*National Preparedness*." This effort is in support of Federal, State, and local response organizations through the Office of Grants and Training.
- Developed in partnership with the U.S. Coast Guard, the U.S. Navy and others, a low cost commercial anti-swimmer system to protect high value assets from underwater attack. This effort was in support of U.S. Coast Guard.
- Tested non-intrusive technologies to quickly inspect shipboard spaces, to locate or inspect hidden compartments for contraband, and technologies to communicate with boarding team members. This effort was in support of U.S. Coast Guard.
- Began support of three efforts to enhance personal protection for U.S. Secret Service personnel: Escape Mask, Handheld Suicide Bomber Detector, and Portable Entry Point Screening Portal for Explosive Detection. This effort was in support of the U.S. Secret Service.

Within the areas of critical infrastructure protection and cyber security, we:

- Established the Cyber Security R&D Center, the S&T Directorate's primary interface with the academic and industrial cyber security research communities.
- Established the Infrastructure Security Program, the goal of which is to develop more secure and robust mechanisms that will enable the Internet to support the Nation's needs now and in the future.

- Established the Cyber Security Testbed Program, which enables a wide community of researchers to explore threats to network security without risk of compromising the actual internet.
- Completed development of software algorithms in coordination with the Electric Power Research Institute for a fast-running modeling and simulation prototype for use in preventing cascading blackouts.
- Published two reports that identified technology aids that significantly close existing operational gaps, to increase the accuracy and reduce the time and cost for personnel background investigations for private security guards and insiders in sensitive positions.
- Issued the first annual National Critical Infrastructure Protection R&D Plan that addressed R&D priorities in the areas of protection and prevention, sensors and detectors, insider threats, social and behavioral issues, and future needs.
- Initiated 11 new projects (bringing our total number of those underway to 22) including rapid prototyping at the Kentucky Critical Infrastructure Protection Institute to support the Department's ability to protect community-based infrastructure.

Within the emerging threats and rapid prototyping areas of the S&T Directorate, we:

- Evaluated the compounded infrastructure threat by investigating ways in which infrastructure (i.e., planes into buildings, nuclear plants, chemical plants) could be used as a weapon. The effort was used to discover and identify those infrastructures not previously viewed as concerns.
- Initiated the Rapid Technology Application Program (RTAP) to expeditiously provide needed new technologies to Federal, State and local components of the homeland security mission. End-users have generated 28 urgent rapid prototyping requirements including the need for specialized personal protective equipment, rapid biological screening tools, portable explosive trace detectors, and systems to immediately locate emergency responders in the field.

Within other areas of the S&T Directorate, we:

- Established the National Science and Technology Threat Awareness and Reachback (NSSTAR) system to provide real time, technical analysis and support to the homeland security community for anticipating, preventing, and responding to chemical, biological, radiological, nuclear, and high explosive (CBRNE) threats.
- Established an Institute for Discrete Sciences (IDS) to investigate and develop the specialized computing algorithms and hardware architectures necessary to analyze massive amounts of diverse data from multiple, disparate, distributed

data sources and to model terrorist attacks and simulate consequences on a real-time, high-resolution basis.

- Completed an engineering design for the Enhanced International Travel Security (EITS) system, which allows the validity of travel documents and the identity of travelers to be determined in real time at U.S. borders and other points of entry.
- Created the Interagency Center for Applied Homeland Security Technology (ICAHST) to enable collaboration among intelligence and law enforcement community agencies on the testing, evaluation, and prototyping of information analysis and sharing technologies.
- Established Regional Communications Interoperability Pilot (RCIP) projects in Nevada and Kentucky. These pilots focused on developing models for improved communications and interoperability to address challenges faced nationwide.
- Established two additional DHS Centers of Excellence at national universities: the National Center for the Study of Terrorism and Responses to Terrorism, and the Center for the Study of High Consequence Event Preparedness and Response. This brings the total number of such university based national centers to five.
- Supported approximately 300 undergraduate and graduate students in DHS mission-relevant fields through the Scholars and Fellows Program, as well as funded postdoctoral scientists and engineers to perform advanced research in areas of critical importance to DHS.
- Integrated two competing Counter-Man Portable Air Defense System (MANPADS) prototypes with planned airframes and performed on-board ground and flight testing to verify system performance and continued air worthiness of the aircraft with the countermeasure system installed.
- Updated SAFECOM's coordinated grant guidance that outlines eligibility requirements, the purposes for which grants may be used, and the guidelines for implementing a wireless communication system. SAFECOM is a communications program that provides RDT&E, guidance, tools, and templates on communications-related issues to local, State, and Federal public safety agencies.
- Prepared the survey tools for the Interoperability Baseline Study, which will provide a quantitative National assessment of public safety communications interoperability.
- Prepared a revised application kit for the *Support Anti-terrorism by Fostering Effective Technologies Act of 2002*, known as the SAFETY Act, that is easier to use and understand, with examples to assist applicants.
- Processed more than 260 pre-applications and 134 unique technology applications under the SAFETY Act. As of Jan. 5, 2006, we granted Designation and Certification to 41 qualified anti-terrorism technologies. An additional 16 technologies have been granted "designation only" status.

FY 2006 ACTIVITIES

As the S&T Directorate matures, we have continued to reevaluate and reassess our priorities to better facilitate capabilities needed by the Department and other customers to make information and analysis sharing possible, to protect the Nation's borders and critical infrastructure, and to ensure that technical and operational solutions enable Federal, State, and local emergency personnel to anticipate, respond to, and recover from attacks on the United States. Just as the Nation's science and technology capabilities have helped us defeat enemies overseas in the past, so too will they help the Nation defeat future efforts of terrorists to successfully attack and disrupt the American way of life. To prepare the Nation to counter threats from weapons of mass destruction as well as natural disasters, the FY 2006 budget request included increase for initiatives that supported R&D to mitigate these weapons and their potentially devastating effects as well as efforts aimed at leveraging technology to produce rapid advances in capabilities to enable DHS personnel to protect the homeland more efficiently and effectively across many components.

Our major ongoing FY 2006 initiatives are aimed at mission-critical areas and problem sets. Some highlights include:

- **National Bio and Agrodefense Facility (NBAF) –** The proposed NBAF is envisioned to provide the Nation with the first integrated agricultural, zoonotic disease, and public health RDT&E facility with the capability to address threats from human pathogens, high-consequence zoonotic disease agents, and foreign animal diseases. This supports the complementary missions of DHS, the Department of Human Health and Services (HHS) and the United States Department of Agriculture (USDA). NBAF will provide new RDT&E infrastructure that will allow for research to enhance agricultural and public health. This capability is needed to fill a critical gap in the Nation's agro and biodefense plan. The NBAF would enhance the national biodefense complex by modernizing and integrating agriculture biocontainment laboratories for foreign animal disease, human pathogens, and zoonotic diseases through Biosafety Level (BSL) 3 Agricultural and BSL 4 laboratory spaces. It will also provide the additional infrastructure required for threat and vulnerability assessments and for testing and evaluating promising foreign animal disease countermeasures. Development of an integrated, national bio and agrodefense strategy has revealed that the current capabilities are inadequate to meet future research requirements supporting both agricultural and public health national security. Foreign animal disease studies, public health threats from emerging, high-consequence zoonotic pathogens, and the need for development and licensure of medical countermeasures, are generating additional demands for biocontainment laboratory space. Current laboratory space available in the United States is not sufficient to support the increasing levels of research, development, and testing needed to meet the growing concerns about accidental or intentional introduction of foreign animal diseases into this country. DHS

issued an Expression of Interest (EOI) on January 19, 2006, to solicit interest for potential sites for the NBAF facility. The EOI will solicit input from organizations or consortia of Federal agencies, State and local governments, industry, and academic institutions. In addition to the EOI, the S&T Directorate plans to release a request-for-proposals in February 2006 to procure architect-engineer services to conduct conceptual design studies for the NBAF.

- **Low Volatility Agent Warning System –** Develop the Low Volatility Agent (LVA) Warning System to serve as the basis for a warning and identification capability against a set of chemical threat agents whose vapor pressure is sufficiently low that detection by conventional approaches is exceptionally difficult. This set of low volatility agents includes some of the most toxic materials currently known. The Chemical Countermeasures Portfolio has initiated an effort to develop a transportable capability for the detection of these materials in a response and recovery mode—the LVA Surface Contamination Monitor. The FY 2006 funding is being used to develop a protection-mode capability to detect these materials upon release in specific environments. This detect-to-warn system will alert the response system of the imminent hazard thereby enabling protection of potential victims from exposure and permitting application of prompt medical countermeasures to minimize or eliminate casualties. This system will be a network of detectors to provide a protect-to-warn capability for specific venues, such as high-value buildings and transit systems. The LVA Warning System will both detect and identify the agent to ensure correct medical countermeasures are engaged.

- **Counter-MANPADS –** Based on the Phase II results in FY 2006, the Counter-MANPADS Program will initiate Phase III to conduct operational test and evaluation on Counter-MANPADS advanced prototype equipment installed on commercial aircraft operated by U.S. cargo carriers. The primary objective is to reduce the residual risk of operations in the commercial environment and lower the cost of ownership. To maintain competition between two different approaches to design and integration, the Counter-MANPADS Program will maintain two contractors in Phase III. In FY 2006, each contractor will update its designs to incorporate enhancements for reliability improvements, technology protection, and emergency ground notification. Operational testing and evaluation will be performed on multiple aircraft types to capture true operations and maintenance costs, as well as technical performance and reliability data. In FY 2006, eight operational test aircraft will be modified and nine Counter-MANPADS systems will be procured to support reliability developments, test data collection, and critical technology protection measures. Additionally, live fire test evaluations will provide insight into the overall effectiveness of the system installed on commercial aircraft. Finally, Federal Aviation Administration (FAA) certification will be completed for additional relevant aircraft types, models and series not addressed in Phase II.

- **Research and Development Consolidation –** The consolidation of the Department's R&D efforts will continue to be an ongoing priority for the S&T Directorate. We will continue working with the Transportation Security

Administration, CBP and others to solidify integration of their RDT&E activities into the S&T Directorate. This consolidation is bringing the scientific and engineering personnel and other RDT&E resources of the Department under a single accountable authority.

FY 2007 PLAN

In FY 2007, the S&T Directorate will maintain ongoing activities in science and technology research to detect and counter threats and attacks; protect the Nation's critical infrastructure, both physical and cyber; analyze and assess threats and vulnerabilities; and provide cutting edge technologies to operational end-users. We will support the Department's strategic goals and objectives by performing RDT&E while addressing the following criteria:

- *Risks facing the Nation* that are identified and weighed by the S&T Directorate and others, including DHS's Office of Intelligence Analysis;
- *Homeland security needs* that are identified through a systematic science and technology needs identification process that the S&T Directorate conducts with its partners;
- *Estimated costs, benefits, implementability, and potential effectiveness* of results of science and technology research and programs*;* and
- *DHS's overall priorities,* since the S&T Directorate supports and enables DHS's overall homeland security efforts.

To accomplish these goals, the S&T Directorate proposes a total budget of $1.0 billion and 383 full-time equivalent employees (FTEs). The "Management and Administration" request is for $195.9 million and provides the resources for the salaries and benefits of the S&T Directorate's employees in support of our homeland security R&D programs. The request for the "Research, Development, Acquisition and Operations" appropriation is $806.4 million.

The FY 2007 President's budget for the S&T Directorate provides the Department with the resources necessary to continue and advance our efforts to develop and deploy the technologies required to enhance the security of the homeland in the 21st century.

Program increases proposed in the FY 2007 President's budget include:

- $7.1 million is requested for the Cyber Security program to enhance efforts in the areas of Domain Name Infrastructure, Secure Protocols for Routing Infrastructure, Cyber Security Testbed development, Large-scale Network Datasets, and Highly Scalable Identity Management.
- $2.0 million is requested to establish a Joint Agro-Terror Defense Office (JADO). The Department's agrodefense responsibilities are defined in several public laws and Homeland Security Presidential Directives, including: the Homeland Security Act of 2002; *Critical Infrastructure Identification, Prioritization, and Protection* (HSPD-7); *Defense of United States Agriculture*

and Food (HSPD-9); and *Bio-defense of the 21st Century* (HSPD-10). The JADO will be led by an executive director who will lead an interagency staff. The JADO will be responsible for coordinating development and deployment of the integrated government-wide agro-defense programs called for by these directives and law.

- $1.0 million to comply with the requirements of Public Law 108-330, the *DHS Financial Accountability Act* which requires the annual Performance and Accountability Report to include an assurance by the Secretary of the adequacy of financial reporting controls. These funds are a critical component of the Department's efforts to prevent waste, fraud and abuse and enhance its financial accountability.

In addition, the FY 2007 S&T Directorate budget proposes the realignment of approximately $110.0 million from the S&T Directorate's "Research and Development" appropriation account to the "Management and Administration" appropriation account. This realignment of funds is proposed to more accurately reflect the fact that in the past, these funds have been used to support the direct and indirect management, administration, and oversight costs associated with the Department's science and technology enterprise. Furthermore, it will provide the Congress and other interested parties with a more transparent view into the S&T Directorate's operations, the distribution of planned and actual expenditures between research and development activities, and the direct and indirect costs associated with their delivery.

RDT&E PROCESS

As I stated one year ago, the S&T Directorate developed an RDT&E process to provide a clearly defined, replicable method for assessing needs and risk, planning, allocating resources and executing programs to produce high-impact, cost-effective and critically needed homeland security technology solutions. We are in the process of streamlining this process to address our programmatic needs. We will use this process to carry out risk-based planning.

SCIENCE AND TECHNOLOGY DIRECTORATE ORGANIZATION

The S&T Directorate is the research and development component of the Department of Homeland Security. The S&T Directorate organizes the vast scientific and technological resources of the United States to prevent or mitigate the effects of catastrophic terrorism against us or our allies. It unifies and coordinates much of the Federal government's efforts to develop and implement scientific and technological countermeasures to terrorist threats. The S&T Directorate is a technically robust, agile, and responsive organization capable of meeting all of its current and future roles and responsibilities in the Department. The four elements of the S&T Directorate are:

- Office of Plans, Programs, and Requirements (PPR);

- Homeland Security Advanced Research Projects Agency (HSARPA);
- Office of Research and Development (ORD); and
- Office of Systems Engineering and Development (SED).

The S&T Directorate implements its science and technology activities through focused portfolios (organizationally within PPR) that address biological, chemical and explosive threats; support the research and development needs of the operational components of the Department; support Federal, State, local and tribal preparedness and infrastructure protection; and cross-cut areas such as standards, threat awareness, and interoperability that impact all aspects of the S&T Directorate's RDT&E process. These portfolios cut across the four elements of the S&T Directorate and integrate the innovative input from private industry and academia as well as national and Federal laboratories. In particular, PPR provides the requirements and technical vision for the S&T Directorate and its RDT&E process. HSARPA has an essential role in meeting the goals and objectives of the Department and the S&T Directorate, through research and development, and technology maturation in industry and academia. ORD executes the S&T Directorate's RDT&E programs within the national and Federal laboratories; establishes the University Centers of Excellence; and maintains the Nation's enduring research and development complex dedicated to homeland security. SED oversees the transition of large-scale and pilot systems to the field through program offices, which bring mature technologies from the laboratory to the user through a rapid, efficient, and disciplined project management process. In addition, the S&T Directorate houses the Office of Weapons of Mass Destruction Operations and Incident Management to offer scientific advice and support to meet operational needs. Through this office, the S&T Directorate exercises its scientific and technical leadership role under the *National Response Plan*.

Portfolios

Biological Countermeasures

The Biological Countermeasures Portfolio provides the understanding, technologies, and systems needed to anticipate, deter, protect against, detect, mitigate, and recover from biological attacks on this Nation's population, agriculture or infrastructure. Biological threats can take many forms and be distributed in many ways, and we take an integrated systems approach to countering them. Our principal areas of interest include: vulnerability and risk analysis to identify the need for vaccines, therapeutics, and diagnostics; development and implementation of early detection and warning systems to characterize an attack and permit early prophylaxis and decontamination; and development of a national bioforensic analysis capability to support attribution of biological agent use. Simulation, modeling, and gaming form an important part of this effort. They help guide and prioritize technical developments, and they are invaluable in training decision makers before and during an event. The Directorate's partners include the Department of Health and Human Services (HHS), the Department of Defense (DOD), the Department of Agriculture (USDA), the Environmental Protection Agency (EPA), the Department of Justice (DOJ), the Department of State (DOS), the United States Postal Service (USPS), and State and local operational end users.

Chemical Countermeasures
The Chemical Countermeasures Portfolio enhances the Nation's capability to anticipate, prevent, protect from, respond to, and recover from chemical threat attacks through interagency leadership and innovative research, development, and technology transition. Our objectives are to enable comprehensive understanding and analyses of chemical threats in the domestic domain; to develop pre-event assessment, discovery, and interdiction capabilities for chemical threats; to develop capability for warning, notification, and timely analysis of chemical attack; to optimize technology and process for recovery from chemical attacks; and to enhance the capability to identify chemical attack sources. Our work reflects our recognition of the need to prepare against a range of threats—classical chemical warfare agents (CWA), toxic industrial chemicals (TICs), and non-traditional agents (NTAs). Coordination with other agencies like the EPA, HHS, the Federal Bureau of Investigation (FBI), DoD, the interagency Technical Support Working Group (TSWG), and the Intelligence Community (IC) remains critical to support our national chemical preparedness goals. The DoD has developed a particularly strong chemical defense program over a number of decades, and is a key partner for moving new capabilities into the domain of homeland security.

Explosives Countermeasures
The Explosives Countermeasures Portfolio develops and coordinates technical capabilities to detect, interdict, and mitigate the consequences of the use of improvised explosives devices (IEDs) in terrorist attacks against U.S. citizens and critical infrastructure. RDT&E activities include prioritization of efforts among the many possible terrorist threats and targets, development of new detection technologies, and evaluation of integrated protective systems for high-value facilities. Our priorities focus on the detection of vehicle bombs, suicide bombers, and leave-behind bombs. As a result of the R&D consolidation in FY 2006, the Explosives Countermeasures Portfolio will also dedicate significant resources to continue the development of explosives detection and blast mitigation systems for civil aviation security. Consistent with this RDT&E leadership role, the Explosives Knowledge Center initiated in FY 2005, will provide guidance and information to ensure that preparedness capabilities at the Federal, State, local, and tribal levels are updated over time to be consistent with new and emerging technologies and capabilities as well as with the changing and emerging threats.

Threat Awareness
Formerly known as the Threat and Vulnerability, Testing and Assessment Portfolio, the RDT&E activities funded through the Threat Awareness Portfolio primarily support two DHS strategic goals: awareness and prevention. These activities provide the tools and knowledge necessary to meet one of the Secretary's recently announced imperatives to increase preparedness, with particular emphasis on catastrophic events caused by weapons of mass effect, and the requirements delineated in the Department's National Preparedness Goal. Our efforts in this area focus on developing information about the two basic elements of terrorist threat — terrorist capabilties on the one hand, and terrorist motivations and intent on the other — and on providing the advanced information processing tools necessary to rapidly and accurately discover, use, and

share such information. Such tools and methods are intended to enable and enhance Federal, State, and local awareness of a broad range of threats through information fusion and information sharing.

Standards Portfolio
The development, adoption and implementation of standards — providing the basis for ensuring the effectiveness of scientific and technological tools — are critically important for homeland security. Measures of effectiveness for any critical technology or tool include basic function, appropriateness and adequacy for the task, interoperability, efficiency and sustainability. With the mission to develop and coordinate the adoption of national standards and appropriate evaluation methods to meet homeland security needs, the Standards Portfolio cuts across all aspects of the S&T Directorate's mission. Homeland Security standards address metrics for products, services, and guidelines, performance specifications, testing and evaluation protocols, training, certification of equipment and personnel, as well as metrics and quality assurance for deployment of systems. Standards are also an essential component of codes of practice and standard operating procedures. These standards will provide DHS the ability to provide guidance to Federal, State, local, and tribal homeland security entities regarding purchase, deployment, and use of these tools.

Cyber Security
Our Cyber Security R&D investments will yield technologies that improve the security of information and information systems in two complementary ways: through the development of a new generation of cyber security technologies to increase the security of information and information systems, and through the development of tools and methodologies to develop more inherently secure systems. The portfolio also fosters technology transfer and diffusion of federally funded R&D into commercial products and services for private sector applications. This technology diffusion will result in broad-based benefits to the Information Technology (IT) sector and to users of IT among the other critical infrastructure sectors. We coordinate with other Federal agencies through the National Science and Technology Council's (NSTC) Cyber Security and Information Assurance (CSIA) Interagency Working Group [co-chaired by DHS and the Office of Science and Technology Policy (OSTP)], and the InfoSec (Information Security) Research Council. We also collaborate informally with other agencies that share interests in the area of cyber security R&D, including the National Science Foundation (NSF), various organizations within DoD, and the National Institute of Standards and Technology (NIST). We actively pursue opportunities to catalyze additional private sector activity. Such opportunities include public-private partnerships as well as increased cooperation and communication among private sector companies and organizations. Finally, we participate in international efforts to develop common areas of collaboration in cyber security R&D.

Critical Infrastructure Protection
The Critical Infrastructure Protection (CIP) R&D Portfolio effort protects the Nation's critical infrastructure and key assets from acts of terrorism, natural disasters, and other emergencies by developing and deploying tools to anticipate, identify, and analyze

risks, and systems to reduce those risks and the consequences of an event. Funded RDT&E and required coordination efforts in this portfolio have been categorized into four programs: Modeling, Simulation, and Analysis; Protective Security Technologies; the Kentucky Critical Infrastructure Protection Laboratory (KyCIPLab); and development of the annual National CIP R&D Plan, as required by HSPD-7, "Critical Infrastructure Identification, Prioritization, and Protection."

Emergent and Prototypical Technology
Our Emergent and Prototypical Technology Portfolio combines two formerly distinct efforts—Emerging Threats and Rapid Prototyping. The mission of the Emergent and Prototypical Technology Portfolio is to: address the dynamic nature of terrorist threats, as science and technology advancements enable new agents of harm and new ways to employ them; and accelerate, through rapid prototyping, the deployment of advanced technologies to address urgent user requirements. The Emergent Threat Program will anticipate and define potential threats arising from new scientific and technological advances or from terrorists using existing technologies in new or unexpected ways, and will jump-start countermeasures capabilities development. Innovative, crosscutting approaches to anticipating and responding to new and emerging threats will permit us to develop capabilities to thwart them before they are used. This Portfolio uses a four-phased process of Discovery, Analysis, Tests, and Potential Solution.

Since relevant R&D is underway at other agencies and organizations, partnerships with DOE, DoD, HHS, DOJ, USDA, and the Intelligence Community offer great benefits.

Supporting the DHS Components
We have programs dedicated to supporting four specific components within DHS: Border and Transportation, Preparedness and Response, the United States Coast Guard, and the United States Secret Service. I will address each of these below.

Border and Transportation
The Border and Transportation (B&T) Portfolio (formerly Border and Transportation Security Portfolio) develops and transitions capabilities that improve the security of our Nation's borders and transportation systems without impeding the flow of commerce and travel. One of the Department's first priorities is to prevent the entry of terrorists and the instruments of terrorism into the United States while simultaneously ensuring the efficient flow of lawful traffic and commerce. Our Border and Transportation S&T Plan and Roadmap represents the combined work of the S&T Directorate and border and transportation agencies to identify new capabilities needed and to plan how the Department will make technology investments in support of B&T mission objectives.

Preparedness and Response
The S&T Directorate's Preparedness and Response Portfolio (formerly Emergency Preparedness and Response) supports the Department's new Preparedness Directorate and FEMA, whose mission is to improve the ability of the Nation to prepare for, respond to, and recover from catastrophic emergencies both natural and man-made through development and deployment of enabling capabilities. We emphasize large-

scale complex events, especially those involving terrorism. Our research areas include incident management, decision support, response and recovery, and technology integration. Our most important customers are State and local emergency responders, emergency managers, and the public they serve. The emergency response community consists of more than 49,000 separate agencies spread throughout the country. Of approximately 18,000 law enforcement agencies, the overwhelming majority have 24 or fewer sworn officers. Over 85 percent of our Nation's firefighters are volunteers. Enhancing the capabilities of such a vast and diverse community, especially against terrorist threats, requires a rigorous and systematic approach to the development and transition of a broad range of technology solutions. Our work is dedicated to applying the best available science and technology for the safety and security our emergency responders and homeland security professionals so that they can effectively and efficiently perform their jobs – saving lives and restoring critical services.

United States Coast Guard

The United States Coast Guard protects the public, the environment, and U.S. economic interests in the Nation's ports and waterways, along the coast, on international waters, or in any maritime region as required to support national security. The Coast Guard research program supports this mission through the development of technologies and systems to enhance Maritime Domain Awareness (MDA), and to improve Operational Presence and Response. MDA includes all systems, sensors, and command and control systems necessary to detect, identify, and determine the threat potential of all vessel traffic. It also includes Port Security to protect important harbors. Operational Presence and Response involves safely and effectively stopping a vessel, boarding it, and finding or eliminating any threat or contraband. Research and development in this program aims to give the Coast Guard the means of neutralizing threats as far away from potential targets as possible, and of responding to emergencies as quickly and effectively as possible. Coast Guard R&D is characterized by its many partnerships with other Federal agencies and international groups to share costs and expedite delivery of important products. This program also supports such unique and traditional Coast Guard missions as Search and Rescue, Maritime Regulations, and Marine Safety. Research into oil spill prevention and response, and Aquatic Nuisance Species prevention supports the Marine Environmental Protection Program. Development of advanced navigation systems to improve the flow of goods and services via our Nation's waterways also serves a traditional Coast Guard mission.

United States Secret Service

The United States Secret Service (USSS) Portfolio develops and deploys advanced technologies to enhance that agency's protective and investigative capabilities. This portfolio supports the unique USSS mission by developing and deploying advanced technologies to enhance protective and investigative capabilities and has established its first direct-funded R&D program. The Portfolio focuses on input from threat-based models and the lessons learned from direct operational experience.

Programs and Offices

Office for Interoperability and Compatibility

The Office for Interoperability and Compatibility's (OIC) mission is to strengthen and integrate interoperability and compatibility efforts to improve local, tribal, State, and Federal public safety preparedness and response. Non-interoperable, incompatible communications equipment and a lack of standardized operating procedures have plagued the public safety community for decades. Often public safety agencies cannot perform mission-critical duties because they cannot effectively cooperate with other agencies or operate in other jurisdictions. By coordinating and leveraging the Department's interoperability programs and related efforts, OIC reduces unnecessary duplication of effort, identifies and promotes best practices, and coordinates activities related to interoperability. OIC manages programs to address interoperability and compatibility for public safety providers and the larger homeland security community. Initial program areas include communications (including SAFECOM and Disaster Management programs), equipment, training, and other programs (including the Risk Assessment Policy Group).

Counter-MANPADS

The Counter-MANPADS Program focuses on demonstrating the viability, economic costs, and effectiveness of adapting existing military technology to protect commercial aircraft from the threat of shoulder-fired missiles, i.e. MANPADS. Its goal is to integrate and evaluate existing Counter-MANPADS technologies for potential use by the commercial airline industry, not to develop new technologies. The Program balances cost, suitability, and performance to meet the needs of commercial aviation community stakeholders. Suitable countermeasure systems must be capable of being implemented with minimal impact on air carrier and airport operations, maintenance, and support activities. After completing the second of three planned program phases, DHS will provide a report detailing the equipment performance, projected costs, and potential deployment options. The anticipated release date for the report is mid- to late-March 2006.

University Programs

University Programs coordinate, leverage, and use the academic community's immense intellectual capital to address current and future mission-critical homeland security needs, through both research and educational programs. Our goals are: 1) developing the scientific research base necessary to advancing knowledge in homeland security fields; 2) developing a cadre of technical experts within the Nation's workforce who are trained to address current and future challenges in securing the homeland; and 3) ensuring the results of their research are disseminated to DHS and its partners. The University Programs portfolio is invested largely in two areas: a university-based system of DHS University Research Centers, and a Scholars and Fellows Program intended to build and develop the next generation of academic researchers in disciplines that are relevant or essential to homeland security. University Programs is now a catalyst for mission-relevant research at more than 40 major research universities, and is building capacity worldwide by attracting over 150 faculty and their peers, hundreds of graduate and undergraduate researchers, as well as DHS Scholars and Fellows from more than 110 institutions, to focus on issues critical to homeland security.

SAFETY Act

In accordance with criteria set forth in the SAFETY Act of 2002 and Interim Regulations the Office of SAFETY Act Implementation evaluates technologies. As part of the *Homeland Security Act of 2002,* Public Law 107-296, Congress enacted the SAFETY Act to provide "risk management" and "litigation management" protections for sellers of qualified anti-terrorism technologies. The act's purpose is to encourage development and deployment of anti-terrorism technologies, particularly those aimed at preventing, detecting, identifying, or deterring acts of terrorism, or to limiting the harm that such acts might otherwise cause. The SAFETY Act creates certain liability limitations for "claims arising out of, relating to, or resulting from an act of terrorism" where qualified anti-terrorism technologies have been deployed. The office's evaluations are designed to advise DHS leadership on whether to grant SAFETY Act protections to technologies that applicants submit. In order to stimulate the development and adoption of valuable new technologies, the office seeks to raise public awareness of the benefits of the protections available under the SAFETY Act. The office also coordinates with other DHS elements and other Federal agencies to support those offices' missions and minimize the burden on applicants for SAFETY Act protection. This advance coordination regularly occurs in cases where the SAFETY ACT could play a positive role in a pending Federal procurement.

RDT&E CONSOLIDATION

To ensure strategic direction and avoid duplication, the S&T Directorate is charged with consolidating the Department's research and development activities. As I mentioned earlier, we have made significant steps by integrating the Transportation Security Laboratory into the S&T Directorate. We are continuing to further unify and coordinate efforts to develop and implement scientific and technological countermeasures.

In keeping with legislative intent of the *Homeland Security Act of 2002 and the FY 2004 and 2005 Homeland Security Appropriations*, the S&T Directorate, through RDT&E consolidation, seeks to:

- Bring under a single accountable authority, the scientific and engineering personnel and most RDT&E resources of the Department;
- Maximize the efficiency and effectiveness of the Department's RDT&E capacity;
- Develop and expand synergistic RDT&E programs that cut across the Department's activities;
- Create a world class RDT&E capability; and
- Allow the other organizational elements within DHS to focus on their operational missions by eliminating within them the specialized management infrastructure required to manage organic RDT&E.

Major RDT&E consolidation measures in FY 2006:

- TSL in Atlantic City, New Jersey became part of the S&T Directorate in FY 2006. The S&T Directorate has been working closely with TSA to ensure the seamless transition of TSL's staff and research capabilities. A Memorandum of Understanding is guiding the transition of responsibility from TSA to the S&T Directorate for the assets, liabilities, and program capabilities of the TSL and defining a collaborative framework that will minimize the disruption of program work at TSL and prevent the duplication of effort during this transition. The S&T Directorate has been assessing and integrating existing TSL projects into its transportation security and high explosives portfolio strategies as appropriate.
- Funds originally requested by the CBP to support salaries for those assigned to its Research, Development, and Evaluation Branch were likewise integrated into the S&T Directorate mission.

In FY 2007, the S&T Directorate will continue to perform its role as the primary research, development, testing and evaluation arm of the Department.

TECHNOLOGY TRANSFER

Providing operational end users with the technology and capabilities they need to detect and prevent terrorist attacks, the means of terrorism and other illegal activities is the capstone of the S&T Directorate's mission.

To successfully carry out this aspect of our mission, the S&T Directorate actively works to transition cutting-edge homeland security technologies to end-users within the Department, other Federal agencies, State and local government entities, and the private sector. Some recent accomplishments in this area include:

- Regional Technology Integration Initiative (RTII) – In FY 2005, RTII completed integrated community-based vulnerability assessments in four pilot locations. We are currently working with these communities to identify appropriate homeland security technology solutions for the gaps identified. In FY 2006, we are focusing on technology deployments in these four regions and on the transfer of lessons learned to "peer cities." Additional locations may be added in the future as we identify gaps that have not been addressed through the pilot locations. RTII provides the basis for improved preparedness, mitigation, and response by regional authorities, including cities and counties that will result in lives saved and greater effectiveness of disaster management resources. This program is a fundamental transition path for technologies that will help regional authorities across the Nation counter emerging threats.
- DoD's 1401 Program – Pursuant to the direction of Congress to quickly deploy technology where it is needed, DHS is working with DoD and DOJ to identify and transfer current appropriate technology to Federal, State, and local emergency responders for homeland security applications. The 1401 Technology Transfer Program is aimed at efficiently transitioning these

technologies to the broader public safety community. As part of this effort, key interagency stakeholders selected five high-priority technologies from a field of 550 DoD technologies that matched a list of first responder needs. Through the 1401 Program, the S&T Directorate will ensure that technologies transferred to first responders meet standards of interoperability and compatibility with existing public safety operations, and that they are tested and evaluated by first responders. In support of this role, the S&T Directorate OIC sponsored a series of focus groups with public safety practitioners in August 2005 in an effort to validate the function and application of these technologies in their respective environments.

- Technology Clearing House – The S&T Directorate has awarded a contract to the Public Safety and Security Institute for Technology (PSITEC) to provide these services, which will all be available through a Knowledge Portal. When complete, the Knowledge Portal will provide a one-stop-shop for access to relevant information from a wide variety of sources, including the existing Responder Knowledge Base and the Lessons Learned Information Sharing (LLIS) created by the Memorial Institute for the Prevention of Terrorism (MIPT), under sponsorship from the DHS Office of Domestic Preparedness. Its architecture will be open, interoperable, and non-proprietary to facilitate cost effective, long-term operations, maintenance and upgrades.
- Next-Generation Cyber Security Technologies Program – To stimulate transfer of DHS-funded technologies into mainstream commercial products and services, FY 2006 activities emphasize testing, evaluation, and piloting of the most promising technologies emerging from the now completed program that began in FY 2004.

While highlighting these successes, it is important to note that the transfer of technology often requires numerous intricate, incremental steps over many years. Although the basic scientific principles that underpin a particular technology may be leveraged, nevertheless significant re-engineering is required to make the technology suitable for homeland security purposes. In most cases, technology developed for one purpose, such as a military application, may not be able to be transferred in a straightforward manner to civil operations. The requirements for maintenance and support, for performance, and for total cost-of-ownership often must be reengineered or otherwise resolved to permit such transfers.

During the next year, the S&T Directorate will work closely with its government, international and private sector partners to overcome these institutional and technical challenges. In FY 2007, the S&T Directorate plans to continue its technology transfer to end users. Plans include:

- The Facility Restoration Technology Demonstration – This demonstration will focus on the transfer and application of the concepts developed in FY 2005 and FY 2006 for airports to other types of critical facilities such as subway systems and other transportation nodes. In addition, FY 2007 accomplishments will focus on filling data and technology gaps critical to the restoration of facilities

such as the decontamination of sensitive equipment and the interactions of chemical agents on surfaces.

- Technology Clearing House – The Emergent and Prototypical Technology Portfolio will continue to support the Technology Clearinghouse in FY 2007. Development plans include: adding procurement decision support tools and advanced search mechanisms; expanding content to include topics such as public health information; forming communities of interest and professional discussion boards; and establishing a technology transfer community database.

STRATEGIC PARTNERSHIPS

The S&T Directorate places great importance on its interactions with the other Federal departments and agencies that are contributing to the Nation's homeland security science and technology base. We are accustomed to working in an interagency working group mode, and have found this approach to be quite effective in addressing a variety of key areas. To proceed in this current effort, we must have a complete picture of all Federal government components involved in research and development, and regularly utilize the collective wisdom that the interagency process brings to the table. We must understand one another's R&D capabilities and current activities and plans, both near- and long-term, because only when we have an accurate and comprehensive picture of the current state of the Nation will we be able to effectively develop a roadmap for success.

Only through increased communication and partnering are we able to leverage existing Federal resources to sustain the science and technology advances essential to homeland security. These advances in turn provide security solutions that are technically, economically, and socially sustainable. This superior technical base continuously enables the United States to stay ahead of the changing threats and escalating abilities of our adversaries.

Research and development needed to enhance the Nation's capabilities to thwart terrorist acts and mitigate natural disasters is being conducted by the Department of Commerce (DOC), USDA, DoD, DOE, DOJ, HHS, DoS, and Veteran's Affairs as well as within the National Science Foundation (NSF), EPA, other Federal agencies.

By bringing these organizations together through strategic partnerships, we are creating an enduring homeland security science and technology community. As directed by the *Homeland Security Act of 2002*, the S&T Directorate is continuing to solidify this community by coordinating the Federal government's civilian efforts to identify and develop countermeasures against current and emerging threats. In support of these efforts during the last year, the S&T Directorate has:

- Worked with the OSTP, the Homeland Security Council, the National Security Council, the Office of Management and Budget and the Office of the Vice

President in the effort to coordinate homeland security research and development across the entire United States Government;

- Led the development of the *National Plan for Homeland Security Science and Technology*. This strategic plan will establish R&D priorities within and across Federal programs and identify opportunities to leverage the R&D efforts of other agencies.
- Established meaningful interagency interactions with Federal, State and local government and private sector entities to meet the high priority homeland security RDT&E needs of the Nation. This includes actively participating in or leading several interagency working groups. Such groups foster an active exchange of information and assist participating agencies in identifying related needs and requirements, conducting research and development of mutual benefit, and avoiding duplication of effort.

Through these and other interagency interactions, the S&T Directorate is bringing together the vast homeland security scientific and technology resources of the Nation. Significant accomplishments and ongoing collaborative efforts from across the S&T Directorate are listed below:

- Biodefense Collaboration – DHS and the S&T Directorate partner with, and support, other Federal departments and agencies with lead responsibilities in biological threats—a major focus of our countermeasure R&D. We are working with the HHS on medical countermeasures and mass casualty response; USDA on agriculture biosecurity and food security; and EPA on decontamination and water security including a jointly funded center for microbial risk assessments. In a major initiative, S&T is collaborating with other Federal partners to establish the National Interagency Biodefense Campus, which includes our partnership with the DoD on the National Biodefense Analysis and Countermeasures Center (NBACC). This Center will provide the Nation with cutting edge capabilities in bioforensics and biological threat characterization. S&T and DoD's Defense Threat Reduction Agency (DTRA) are collaborating on BioNet, a program to integrate military and civilian biomonitoring activities and establish a shared communications process to provide timely biothreat information. The S&T Directorate maintains a close liaison with the DOS on matters relating to the Biological Weapons Convention (BWC) which is essential to DHS biological countermeasure programs and compliance posture.
- Chemical Countermeasures Collaboration – The S&T Directorate is working with DoD to plan a Chemical Security Analysis Center (CSAC) that will serve as a knowledge management, threat characterization, and forensic analysis hub that will address a full range of chemical threats, particularly chemical warfare agents and non-traditional agents. We are also coordinating with HHS' Centers for Disease Control (CDC) and the EPA on the larger Chemical Laboratory Response Network (CLRN). In the aftermath of Hurricane Katrina, we have already seen how components of CLRN will produce a more coordinated, more effective laboratory response effort. The CDC activated the Laboratory

Response Network to conduct sampling and analysis for identification of toxic chemicals and pathogens in Gulf Coast areas.

- Critical Infrastructure Protection – Under HSPD-7, *Critical Infrastructure Protection,* DHS is assigned the overall responsibility for coordinating the national effort to ensure the security of the Nation's critical infrastructure and key resource sectors. Per this directive, the S&T Directorate is working with the Chemical Sector Coordinating Council, comprised of 16 key stakeholders, to draft the Nation's strategic vision for better securing the chemical sector infrastructure. Our key Federal partners in chemical security include DoD, HHS, the FBI, the EPA, and the interagency Technical Support Working Group (TSWG). In addition, we established the Process Control Systems Forum (PCSF) to develop new cross-industry guidelines, protocols and system architecture for provably secure, next-generation Supervisory Control and Data Acquisition (SCADA) and related types of process and distributed control systems. PCSF is comprised of government and private industry stakeholders, owners, and operators.

- Maritime – The Science and Technology Directorate's Coast Guard R&D program is characterized by its many partnerships with other Federal agencies and international R&D groups. Beyond the program support for the Coast Guard's traditional missions, we have ongoing collaborations in the maritime security domain. We are supporting the Department's participation in a broad maritime security program review looking at all current U.S. government maritime policy initiatives and ensuring interagency alignment to guide a focused national effort to improve Maritime Domain Awareness. Maritime Domain Awareness includes all systems, sensors, and command and control systems necessary to detect, identify, and determine the threat potential of all vessel traffic. It also includes Port Security to protect important harbors. In accordance with National Security Presidential Directive 41 and HSPD-13, "Maritime Security Policy," issued last December, DoD and DHS are leading an interagency initiative to develop the National Strategy for Maritime Security. The S&T Directorate is supporting that effort as well as the ongoing comprehensive National Maritime Response Plan that clarifies lead agency roles and responsibilities regarding maritime threats.

- Transportation Security Partnerships – The S&T Directorate works in close cooperation and collaboration through a Cargo Security Integrated Planning Process Team (IPPT) process. The IPPT is co-chaired by S&T and the DHS Policy Office, and has representatives from within the Department as well as the Departments of State, Commerce, Defense, Transportation and Energy. Through this IPPT, DHS actively ensures coordination with existing government programs and leverages those relationships to foster a cohesive program strategy and avoid the duplication of effort. Other transportation security efforts focus on Freight Rail Security with the Federal Railroad Administration and the S&T Directorate's ongoing Counter-MANPADs program. In partnership with other Federal agencies (FAA, DoD, DOS), the S&T Directorate initiated a Congressionally-directed aggressive System Development and Demonstration

program to counter the threat of shoulder-fired missiles. The program demonstrates and evaluates the possible migration of existing military Counter-MANPADS technologies to the commercial airline industry.

- Border Security – Over the past three years, the S&T Directorate has coordinated extensively with DoD, the National Aeronautics and Space Administration (NASA), and FAA with respect to Unmanned Aerial Vehicle (UAV) operations and evaluations for the U.S. Border Patrol. The UAV Executive Steering Group was established to advise the Secretary of Homeland Security and provide a forum for communication, coordination and cooperation. The UAV Executive Steering Group is made up of representatives from DHS components, DoD and the FAA.

International Partnerships

The S&T Directorate recognizes the enormous benefits gained from working with the international community to seek technology solutions to our common homeland security problems. We have worked in concert with our Federal government agency counterparts to both negotiate agreements with key foreign partners and to implement strategic programs under those agreements that meet our mutual high-priority needs.

The S&T Directorate is currently the United States' lead agency for umbrella S&T Agreements that have been created with Canada, the United Kingdom, and most recently with Australia. These instruments provide the mechanism for us to share resources, ideas, and information in order to leverage our individual investments, to benefit from each other's experiences and perspectives of others, and also importantly to create consistency in the tools and systems that we ultimately field. We are taking advantage of the opportunities presented by these partnerships across the entire suite of civil security mission requirements.

Cooperative research, development, testing and evaluation activities are being pursued with other countries as well. In particular, we are looking at ways to enhance an already robust collaboration with Israel, especially in testing of explosives detection and mitigation technologies in operational environments. As part of the Security and Prosperity Partnership initiative, we have reached out to Mexico to begin a dialog on technology to address agricultural security. We understand the need to engage foreign entities on technology issues around travel and trade security and have initiated interactions with Singapore, the Netherlands, Sweden and Japan in this arena.

CONCLUSION

In conclusion, I thank you for the opportunity to appear before you today. I can assure you that we are on-task, and that we are providing the planners, operators, and responders we serve with the best support our science can offer. Homeland security continues to benefit tremendously from the work of our Nation's scientists and engineers. The knowledge, the systems, the methods, and the tools they give us do much to make us safer and more prepared.

On behalf of all of us in the Science and Technology Directorate, I thank you for your continuing support and counsel. I am proud of what we have been able to accomplish in just a few years, and I trust we will continue to live up to the responsibility the Nation has given us. I will be happy to answer any questions that you may have.