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 Appropriations
Subcommittee on Homeland Security

March 30, 2004

Table of Contents

Introduction 3
Science and Technology Directorate Organization 4
Office of Plans, Programs and Budgets 4
Office of Research and Development 5
Homeland Security Advanced Research Projects Agency 5
Office of Systems Engineering and Development 6
Office of Weapons of Mass Destruction Operations and Incident Management 6
Results from Current Research and Development (R&D) Spending 6
Biological Countermeasures 8
Chemical Countermeasures 9
High Explosives Countermeasures 10
Radiological and Nuclear Countermeasures 11
Threat and Vulnerability, Testing and Assessment 12
Standards 13
Emerging Threats 14
Rapid Prototyping 15
Support to Department of Homeland Security Components 15
Support to Border and Transportation Security 16
Support to Emergency Preparedness and Response 16
Support to United States Coast Guard 17
Support to the United States Secret Service 17
Homeland Security University and Fellowship Programs 18
Counter-MANPADS 18
SAFECOM 19
Prioritization 20
Division of Effort Among the DHS S&T Directorate and Research Efforts at Other Government Agencies 20
Outside Inputs to the S&T Budget 22
Metrics Developed by the Science and Technology Directorate 22
Short-Term and Long-Term Research 27
Rationale for Budget Increases: BioWatch and the National Biodefense Analysis and Countermeasures Center 28
Transfer of R&D Budgets and Activities from Other Directorates 29
Budget and Activities Supporting Cybersecurity R&D 31
Basis for Policy on the Use of the National Laboratories 31
Budget for University Centers of Excellence and Fellows Programs 32
Staffing 33
Conclusion 33
Appendix 34

Introduction

Good morning. Chairman Rogers, Congressman Sabo, and distinguished Members of the subcommittee, it is a pleasure to be with you today to discuss the research and development activities of the Department of Homeland Security's Science and Technology Directorate.

The Nation's advantage in science and technology is key to securing the homeland. The most important mission for the Science and Technology Directorate is to develop and deploy cutting-edge technologies and new capabilities so that the dedicated men and women who serve to protect and secure our homeland can perform their jobs more effectively and efficiently – these men and women are my customers.

When I last reported to you about our activities, we had just started our work. Since its inception less than a year ago, the Science and Technology Directorate has:

1) deployed continuously operating biological pathogen detection systems to approximately 30 United States cities;
2) set up testbeds for radiation and nuclear warnings at air and marine cargo ports in cooperation with the Port Authority of New York and New Jersey,
3) established the first series of interoperability guidelines for the Nation's wireless emergency communications network;
4) established the first national standards guidelines for radiation detection equipment;
5) adopted its first standards regarding personal protective equipment developed to protect first responders against chemical, biological, radiological and nuclear incidents.
6) awarded the first Homeland Security Fellowships and Scholarships;
7) established the first Homeland Security University Center of Excellence,
8) transferred the Plum Island Animal Disease Center from the Department of Agriculture to the Science and Technology Directorate;
9) engaged private industry in bringing innovative and effective solutions to homeland security problems through the interagency Technical Support Working Group and issuance of HSARPA's first two Broad Agency Announcements and a Small Business Innovative Research Program solicitation;
10) initiated a development and demonstration program to assess the technical and economic viability of adapting military countermeasures to the threat of man portable anti-aircraft missiles for commercial aircraft;
11) collaborated with and assisted other components of the Department to enhance their abilities to meet their missions and become active contributors in interagency working groups — all while staffing this Directorate with some of this country's brightest and most dedicated people.

I continue to be energized by and proud of the scientists, engineers, managers, and support staff in the Science and Technology Directorate. We have accomplished a great

deal in a short amount of time and are positioning the Directorate to make continuing contributions to the homeland security mission of the Department.

However, the threats to our homeland remain diverse and daunting. We must constantly monitor current and emerging threats and assess our vulnerabilities to them, develop new and improved capabilities to counter them, and mitigate the effects of terrorist attacks should they occur. The Science and Technology Directorate must also enhance the conventional missions of the Department to protect and provide assistance to civilians in response to natural disasters, law enforcement needs, and other activities such as maritime search and rescue.

Science and Technology Directorate Organization

Because our Department is relatively new, I'd like to describe the way we are structured. We have four key offices in the Science & Technology Directorate, each of which has an important role in implementing the Directorate's Research, Development, Test, and Evaluation (RDT&E) activities. Individuals with strong credentials have been appointed to head each office and we continue to strategically add highly skilled technical, professional and support staff. These offices are: Plans, Programs and Budgets; Research and Development; Homeland Security Advanced Research Projects Agency; and Systems Engineering and Development. In addition, we have created the Office of Weapons of Mass Destruction Operations and Incident Management to offer scientific advice and support.

Crosscutting the four key offices, the Science and Technology Directorate is implementing its activities through focused portfolios that address biological, chemical, high explosives, radiological and nuclear, and cyber threats; support the research and development needs of the operational units of the Department; support the development of standards; develop an enduring R&D capability for homeland security; and receive valuable input from private industry and academia as well as national and Federal laboratories. I will talk about the offices first and then about the portfolios.

Office of Plans, Programs and Budgets

The Office of Plans, Programs and Budgets operates under the supervision of Dr. Penrose Albright. He has organized this office into the portfolios I just mentioned, each of which is focused on a particular discipline or activity; taken together, these portfolios span the Directorate's mission space. As I will cover the portfolios in detail later in this testimony, I will limit myself here to a summary explanation. The staff of each portfolio is charged with being expert in their particular area; with understanding the activities and capabilities extant in Federal agencies and across the broad research and development community; and with developing a strategic plan for their particular portfolio, to include near-, mid-, and long-range research and development activities. In addition, we have staff that is charged with understanding the threat from a technical perspective, with integrating the various portfolios into a coherent overall plan, and with developing the corresponding budget and monitoring its financial execution.

Finally, the Office of Plans, Programs and Budget is responsible for executing the Directorate's implementation responsibilities for the SAFETY (Support Anti-Terrorism by Fostering Effective Technologies) Act.

Office of Research and Development

We are fortunate to have Dr. Maureen McCarthy as our Director of Science and Technology's Office of Research and Development (ORD). Dr. McCarthy has served as Chief Scientist for the National Nuclear Security Administration and the Department of Energy (DOE) and was previously DOE's senior representative to the Homeland Security Transition Planning Office. She will lead the office as it strives to provide the nation with an enduring capability in research, development, demonstration, testing and evaluation of technologies to protect the homeland. This office also plans to provide stewardship to the scientific community and to preserve and broaden the leadership of the United States in science and technology.

Activities within ORD address the resources that can be brought to bear to better secure the homeland through the participation of universities, national laboratories, Federal laboratories and research centers. Directors have been appointed to lead efforts in each of these areas and staff is being added rapidly.

Homeland Security Advanced Research Projects Agency

Dr. David Bolka joined us in September 2003 as director of the Homeland Security Advanced Research Projects Agency, known as HSARPA. Dr. Bolka made significant contributions in advancing technical and scientific projects in his prior work with Lucent Technologies and Bell Laboratories, following a notable career in the United States Navy.

HSARPA is the external research-funding arm of the Science and Technology Directorate. It has at its disposal the full range of contracting vehicles and the authority under the Homeland Security Act to engage businesses, federally funded research and development centers, universities and other government partners in an effort to gather and develop viable concepts for advanced technologies to protect the homeland.

HSARPA's mission, as stated in the Homeland Security Act of 2002, is to support basic and applied homeland security research to promote revolutionary changes in technologies that would promote homeland security; advance the development, testing and evaluation, and deployment of homeland security technologies; and accelerate the prototyping and deployment of technologies that would address homeland security vulnerabilities. Its customers are state and local first responders, and Federal agencies that are allied with homeland security such as the United States Coast Guard, United States Secret Service, the U.S. Citizenship and Immigration Services, the Federal Emergency Management Agency and others.

About 60 percent of the Science and Technology Directorate's appropriation in FY 2004 will be executed directly through the private sector with HSARPA managing about half of that. At least 5 to 10 percent of HSARPA's funds are dedicated for revolutionary, long-range research for breakthrough technologies and systems.

Office of Systems Engineering and Development

Mr. John Kubricky joined us in early October 2003 as our Director of the Office of Systems Engineering and Development (SE&D). He is tasked with leading the implementation and transition of large-scale or pilot systems to the field through a rapid, efficient and disciplined approach to project management. Mr. Kubricky previously served as Advanced Program Development Manager for Northrop Grumman and has held senior positions with California Microwave and Westinghouse Defense.

One of the Science and Technology Directorate's challenges is to evaluate a wide spectrum of military and commercial technologies so rapid, effective and affordable solutions can be transitioned to the Department's customers that include first responders and Federal agencies. In some cases, military technologies could be candidates for commercialization, but rigorous systems engineering processes need to be applied to ensure a successful transition. SE&D's role is to identify and then, in a disciplined manner, retire risks associated with such technologies to ready them for deployment to the field. In doing so, the office must view each technology through the prism of affordability, performance and supportability — all critical to end-users.

SE&D must weigh considerations such as the urgency for a solution, consequences of the threat, safety of the product, and lifecycle support as new products are introduced. Products must be user friendly, have a minimum of false alarms, require little or no training and consistently provide accurate results. SE&D will demonstrate and test solutions before they are released to the field, and will validate that those solutions meet user expectations.

Office of Weapons of Mass Destruction Operations and Incident Management

We created the Office of Weapons of Mass Destruction Operations and Incident Management to serve as the Science and Technology Directorate's technical support for crisis operations. The office provides scientific advice and support to the Office of the Secretary of Homeland Security in assessing and responding to threats against the homeland. This office's activities are primarily focused on the biological, chemical, radiological, and nuclear threats.

Results from Current Research and Development (R&D) Spending and FY 2005 Plans: Portfolio Details

As I have mentioned, the Science and Technology Directorate has organized its efforts into research and development portfolios that span the set of product lines of the Directorate.

Four portfolios address specific terrorist threats:

- Biological Countermeasures
- Chemical Countermeasures
- High Explosive Countermeasures
- Radiological and Nuclear Countermeasures.

Four portfolios crosscut these threats:

- Threat and Vulnerability, Testing and Assessment – this portfolio includes our support to the Information Analysis and Infrastructure Protection Directorate, including our critical infrastructure protection and cybersecurity activities.
- Standards
- Emerging Threats
- Rapid Prototyping

We also have portfolios that support the operational units of the Department (Border and Transportation Security; Emergency Preparedness and Response, United States Coast Guard and United States Secret Service) in both their homeland security and conventional missions.

Our University and Fellowship Programs portfolio addresses the need to build an enduring science and technology capability and support United States leadership in science and technology.

Our most recent program, Counter-MANPADS, is seeking to improve technologies to protect commercial aircraft from the threat of MAN-Portable Air Defense Systems (MANPADS).

In addition, the Science and Technology Directorate is responsible for the management of one of the Presidential E-Government Initiatives, Project SAFECOM. There are tens of thousands of state and local public safety agencies, and 100 Federal law enforcement agencies that depend on interoperable wireless communications. SAFECOM (Wireless Public SAFEty Interoperable COMmunications) is the Federal government's umbrella program for coordinating Federal wireless interoperability efforts. Additionally, SAFECOM partners with Federal agencies, state, local, and tribal public safety organizations to improve the interoperability of our nation's wireless communications through the development of standards. Because it is a government-wide E-Gov initiative, SAFECOM is not a part of the Science and Technology Directorate's FY 2005 budget request. Rather, SAFECOM is currently funded by multiple partner agencies that transfer funds to DHS. The placement of SAFECOM in the Department of Homeland Security's Science and Technology Directorate allows it full access to the scientific expertise and resources needed to help our nation achieve true public safety wireless communications interoperability.

At this time I would like to briefly describe some of our accomplishments to date and our FY 2005 plans. As can be seen in the following chart, we have an overall FY 2005 budget request of $1.039 billion, which is an increase of $126.5 million (13.9 percent) over the FY 2004 levels. The request includes $35 million for construction of facilities. In addition, the increase includes President Bush's request for an additional $65 million dollars to enhance and expand the BioWatch Program.

	FY 2003	FY 2004 less rescission	Proposed FY 2005	Increases/Decreases from FY 2004 to 2005	
BUDGET ACTIVITY	Amount (millions)	Amount (millions)	Amount (millions)	Amount (millions)	Percent Increase
Budget Activity M&A	**0.0**	**44.2**	**52.6**	**8.4**	**19.1%**
Salary and expenses	0.0	44.2	52.6	**8.4**	**19.1%**
Budget Activity R&D	**553.5**	**868.7**	**986.7**	**118.0**	**13.6%**
Bio Countermeasures (incl. NBACC)	362.6	285.0	407.0	**122.0**	**42.8%**
High-Explosives Countermeasures	0.0	9.5	9.7	**0.2**	**2.1%**
Chemical Countermeasures	7.0	52.0	53.0	**1.0**	**1.9%**
R/N Countermeasures	75.0	126.3	129.3	**3.0**	**2.4%**
TVTA (incl. CIP & Cyber)	36.1	100.1	101.9	**1.8**	**1.8%**
Standards	20.0	39.0	39.7	**0.7**	**1.9%**
Components	0.0	34.0	34.0	**0.0**	**0.0%**
University & Fellowship Programs	3.0	68.8	30.0	**-38.8**	**-56.4%**
Emerging Threats	16.8	21.0	21.0	**0.0**	**0.0%**
Rapid Prototyping	33.0	73.0	76.0	**3.0**	**4.1%**
Counter MANPADS	0.0	60.0	61.0	**1.0**	**1.7%**
R&D Consolidation transferred funds	0.0	0.0	24.1	**24.1**	
Total enacted appropriations and budget estimates	**553.5**	**912.8**	**1039.3**	**126.5**	**13.9%**

Biological Countermeasures

Biological threats can take many forms and be distributed in many ways. Aerosolized anthrax, smallpox, foot and mouth disease, and bulk food contamination are among the threats that can have high consequences for humans and agriculture. Our Biological Countermeasures portfolio uses the nation's science base to prevent, protect, respond to and recover from bioterrorism events. This portfolio provides the science and technology needed to reduce the probability and potential consequences of a biological attack on this nation's civilian population, its infrastructure, and its agricultural system. Portfolio managers and scientists are developing and implementing an integrated systems approach with a wide range of activities, including vulnerability and risk analyses 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 activities; and development of a national bioforensics analysis capability to support attribution of biological agent use.

In FY 2003 and 2004, the Biological Countermeasures portfolio:

- Deployed BioWatch to approximately 30 cities across the nation. BioWatch consists of air samplers that detect the release of biothreat pathogens, such as anthrax, in a manner timely enough to allow for effective treatment of the exposed population. In addition, with additional funds provided by Congress in FY 2004, we were able to integrate environmental monitoring data with biosurveillance to provide early attack alerts and assessments. The environmental monitoring activities include not only BioWatch, which provides continuous monitoring of most of our major metropolitan areas, but also targeted monitoring that is temporarily deployed for special national needs, such as a Homeland Security Elevated Threat Level. While serving the primary function of mitigating attacks, both BioWatch and environmental monitoring systems also play a deterrent role, since terrorists could be less likely to attack if they know that defensive systems prevent them from attaining their goals.

- Established the National Biodefense Analysis and Countermeasures Center, which provides scientific support for technical threat information for scientific and other communities including intelligence activities, prioritizes biothreats, and conducts bioforensic analyses for attribution and hence deterrence.

In FY 2005, we will build upon our past work and continue to deploy and improve wide area monitoring systems for urban areas. Under President Bush's new Biosurveillance Initiative, which accounts for most of the FY 2005 increase in funding, additional capability will be implemented quickly in the top threat urban areas to more than twice the current capability. We will be working on decontamination technologies and standards for facilities and outdoor areas, and a National Academy of Science study characterizing contamination risks will be completed in FY 2005. At a smaller scale, we will define requirements for expanded technology in detect-to-warn scenarios relevant to facilities monitoring. At the same time, we will be building our capabilities in the National Biodefense Analysis and Counterterrorism Center (NBACC) and at Plum Island Animal Disease Center (PIADC). At the NBACC, we are focusing first on bioforensics and development of a biodefense knowledge center; for agro-bioterrorism, we are prioritizing countermeasures to foreign animal diseases. We are requesting additional funding in FY 2005 for Plum Island to improve the facilities and security of this important research and development site.

Chemical Countermeasures

The National Research Council Report *Making the Nation Safer* points out that "chemicals continue to be the weapon of choice for terrorist attacks." The large volumes

of toxic industrial chemicals and materials along with the potential for chemical warfare agents and emerging threat agents constitute a broad range of threats that may be applied to virtually any civilian target.

Our Chemical Countermeasures portfolio provides the science and technology needed to reduce the probability and potential consequences of a chemical attack on this nation's civilian population. The portfolio places high priority on characterizing and reducing the vulnerability posed by the large volumes of toxic industrial materials in use, storage or transport within the nation. The research and development activities include prioritization of efforts among the many possible chemical threats and targets, and development of new detection and forensic technologies and integrated protective systems for high-value facilities such as airports and subways. These activities are informed by end-user input and simulated exercises.

Over the past year, our Chemical portfolio completed Project PROTECT — Program for Response Options and Technology Enhancements for Chemical/Biological Terrorism — a program conducted in collaboration with the Washington Metropolitan Area Transit Authority (WMATA). PROTECT, an operational chemical agent detection and response capability, significantly decreases response time, which in the event of an attack will save human lives. PROTECT is deployed in Metro stations and is operated by the WMATA.

In FY 2005, our focus will be on protecting facilities from chemical attacks and controlling the industrial chemicals that may be used for such attacks. Our scientists, working with the Information Analysis and Infrastructure Protection Directorate (IAIP), will complete a detailed end-to-end study of three reference scenarios, to culminate in recommendations for top-level architectures, identification of key gaps, and a "report card" showing present, mid-term (three-year), and long-term (five-plus year) capabilities. We will qualify candidate off-the-shelf sensors for demonstration in an application to facilities protection. We will also address response and recovery. Working with the user community, we will develop first-generation playbooks for responding to the three reference scenarios and develop technical requirements for personal protection equipment.

High Explosives Countermeasures

The High Explosives Countermeasures portfolio addresses the threat that terrorists will use explosives in attacks on buildings, critical infrastructure, and the civilian population of the United States. The Science and Technology Directorate's portfolio is closely coordinated with the activities ongoing in the Transportation Security Administration to ensure that research and development (R&D) activities are complementary, not duplicative. R&D priorities in this portfolio have focused on the detection of vehicle bombs and suicide bombers, and on providing the science and technology needed to significantly increase the probability of preventing an explosives attack on buildings, infrastructure and people.

This portfolio in FY 2005 will develop and field equipment, technologies and procedures to interdict suicide bombers and car and truck bombs before they can reach their intended targets while minimizing the impact on the American way of life. We will complete testing and evaluation of known procedures and commercial off-the-shelf devices applicable to indoor or outdoor interdiction of suicide bombers, and develop a training package for local law enforcement, including recommended equipment and procedures. In addition, we will support the development of new devices to interdict suicide bombers and study the feasibility of using existing detectors to identify explosives in trucks. Finally, we will analyze the costs and benefits of hardening aircraft cargo containers, cargo bays, and overhead bin storage compartments to better withstand the effects of an explosion.

Radiological and Nuclear Countermeasures

Potential radiological and nuclear threats range from the deliberate dispersal of small amounts of radioactive material to the detonation of an improvised or stolen nuclear weapon to an attack on our nuclear power industry. Our Radiological and Nuclear Countermeasures portfolio provides the science and technology needed to reduce both the probability and the potential consequences of a radiological or nuclear attack on this nation's civilian population or our nuclear power facilities.

On August 19, 2003, our Radiological and Nuclear Countermeasures portfolio formally assumed management of the Port Authority of New York and New Jersey radiation detection test bed. The test bed was previously managed by the United States Department of Energy. Following the transfer, we have broadened the project scope beyond testing and evaluating individual pieces of technology to a systems approach, including response protocols and operational concepts. As part of the Science and Technology Directorate's effort, radiation detection sensors will be deployed and operated by Federal, state, and local inspectors and police at land, maritime and aviation venues. By judging the efficacy of deployed systems over time, we will be able to inform future decisions on detection technology R&D investment, deployment of urban monitoring systems, configurations best able to enhance security, and viable ways to defend against a radioactive dispersal device or an improvised nuclear device.

For FY 2005, we plan to leverage our previous technology and capability successes and place a high priority on providing the end-user community with the most appropriate and effective detection and interdiction technologies available to prohibit the importation or transportation and subsequent detonation of a radiological or nuclear device within U.S. borders. Specifically, we will do the following:

- Integrate at least five Federal, state, and local sites into an operational detection system architecture to detect radiological and nuclear threats;

- Establish a test and evaluation capability, and test and evaluate 90 percent of the FY 2005 prototype technologies developed in the portfolio's programs;

- Demonstrate two advanced characterization technologies for crisis response; and

- Demonstrate a prototype for automatic radiological imaging analysis that enhances current imaging systems at one pilot site.

Threat and Vulnerability, Testing and Assessment

Our Threat and Vulnerability, Testing and Assessment (TVTA) portfolio is one of our largest portfolios, and includes our scientific and technical support to the Information Analysis and Infrastructure Protection (IAIP) Directorate. TVTA includes our R&D activities in Critical Infrastructure Protection and Cybersecurity. Activities in this portfolio are designed to help evaluate extensive amounts of diverse threat information; detect and document terrorist intent; couple threat information with knowledge of complex, interdependent critical infrastructure vulnerabilities; and enable analysts to draw timely insights and distribute warnings from the information. This portfolio provides the science and technology needed to develop methods and tools to test and assess threats and vulnerabilities to protect critical infrastructure and enhance information exchange; this portfolio also includes a Biometrics Program and a Cybersecurity Program.

In FY 2004, TVTA:

- Developed and installed an operational component, the Threat-Vulnerability Mapper (TVM), as part of the Threat and Vulnerability Integration System for the Information Analysis and Infrastructure Protection Directorate. The TVM provides counterterrorism analysts with a simple, straightforward way not only to depict the geographic distribution of threats across the United States, but also to search the underlying databases for information on the possible actors, agents, potential severity of attacks, and extent of the vulnerabilities to and effects of such attacks.
- Co-funded the Cyber Defense Technology Experimental Research ("DETER") Network with the National Science Foundation, a $5.45 million, three-year research project to create an experimental infrastructure network to support development and demonstration of next-generation information security technologies for cyber defense. This is a multi-university project led by the University of California at Berkeley.

- Developed a Decision Support System focused on prioritizing investment, protection, mitigation, response, and recovery strategies related to Critical Infrastructure Protection. The initial proof-of-concept began in August 2003 and a case study is being conducted in February 2004. The prototype model will include representation of all 14 critical infrastructure sectors/assets and their interdependencies.

- Developed advanced algorithms for speeding the creation of DNA signatures for biological pathogen detection through the Advanced Scientific Computing

Research and Development program. These discoveries will result in cheaper, faster and more reliable bio-detectors for homeland security.

In FY 2005, TVTA will provide the science and technology capabilities and enduring partnerships needed to develop methods and tools to test and assess threats and vulnerabilities to protect critical infrastructure and enhance information exchange. The Threat-Vulnerability Mapper is only one component of a large Threat and Vulnerability Information System that we will continue to build, drawing upon advances in the information and computer sciences as well as innovative analytic techniques. Our objective is to continually improve an analyst's capability to answer threat-related questions. The Science and Technology Directorate will contribute to the capability to produce high-quality net assessments and assessments of weapons of mass destruction. We will develop advanced computing algorithms in support of improved aerosol dispersion models, blast effects calculations, neutron interrogation models, bioinformatics, and scalable information extraction; improved algorithms make more accurate information available faster. We will continue to provide, in collaboration with other relevant organizations, the science and technology and associated standards needed in the development of biometrics for precise identification of individuals and develop instrumentation to aid authorized officials in detecting individuals with potentially hostile intent. In the cybersecurity area, the DETER Network testbed will be up and running, and we will competitively fund several low-cost, high-impact solutions to specific cybersecurity problems.

Standards

Ensuring that standards are created and adopted is critically important for homeland security. We need consistent and verifiable measures of effectiveness in terms of basic functionality, appropriateness and adequacy for the task, interoperability, efficiency, and sustainability. Standards will improve the quality and usefulness of homeland security systems and technologies. Our Standards portfolio cuts across all aspects of the Science and Technology Directorate's mission and all threats to improve effectiveness, efficiency, and interoperability of the systems and technologies developed, as envisioned in the Homeland Security Act.

Our Standards portfolio continues to actively engage the Federal, state, and local first responders to ensure that developed standards are effective in detection, prevention, response, management, and attribution. This portfolio also conducts the essential activities in order to meet the requirement of the SAFETY (Support Anti-Terrorism by Fostering Effective Technologies) Act in developing certification standards for technologies related to homeland security.

In FY 2004, our Standards portfolio:

- Created initial standards guidelines, with formal standards nearing completion, for radiation pagers, hand-held radiation dosimetry instruments, radioisotope identifiers and radiation portal monitors. These standards were developed under

the auspices of the American National Standards Institute's Accredited American Standards Committee on Radiation Instrumentation.

- Adopted its first set of standards regarding personal protective equipment developed to protect first responders against chemical, biological, radiological and nuclear incidents. These standards, which will assist state and local procurement officials and manufacturers, are intended to provide emergency personnel with the best available protective gear. These standards result from an ongoing collaboration with the Office of Law Enforcement Standards at the National Institute of Standards and Technology.

- Published guidelines for interoperable communications gear**.** Common grant guidance has been developed and incorporated in the public safety wireless interoperability grant programs of both the Department of Justice and the Department of Homeland Security;

- Launched the SAFETY Act process for evaluating anti-terrorism technologies for potential liability limits.

In FY 2005, the Standards portfolio will continue to work on many fronts and with many partners to establish needed standards for technologies (including equipment), processes, and systems. We will especially focus on two major milestones. First, we will establish technical standards and test and evaluation protocols for decontamination technologies and analysis across the ranges of weapons of mass destruction. Second, we will publish a "Consumer's Report" on radiation and bioagent detection devices for Federal, state, and local users.

Emerging Threats

It is truly the threats we do not yet know that are often the most terrifying. Our Emerging Threats portfolio addresses the dynamic nature of terrorist threats, as science and technology advancements enable new agents of harm and new ways to employ them. This portfolio places high priority on developing the capability to use innovative, crosscutting, out-of-the-box approaches for anticipating and responding to new and emerging threats. Successful identification of emerging threats will permit capabilities to be developed to thwart these emerging threats before they are used.

Relevant R&D is underway at other agencies and organizations; thus, partnerships in this area hold great potential for synergistic focus on homeland security. Work is being done and will continue to be pursued in partnership with the Departments of Energy, Defense, Justice, and Agriculture, the intelligence community, and the National Institutes of Health.

In FY 2003 and 2004, our scientists in the Emerging Threats portfolio established informal partnerships with the intelligence community and with the United States Secret Service in order to leverage ongoing activities in support of over-the-horizon assessment.

In FY 2005, we will leverage the activities started during FY 2004, and continue to focus on developing the capability to use innovative, crosscutting, out-of-the-box approaches for anticipating and responding to new and emerging threats and to develop revolutionary technologies to combat them.

Rapid Prototyping

By accelerating the time needed to develop and commercialize relevant technologies, the Science and Technology Directorate will ensure that operational end-users will be better able to prevent terrorist attacks, reduce the nation's vulnerability, and minimize the damage and assist in recovery if attacks occur. Our Rapid Prototyping portfolio advances the Directorate's mission to conduct, stimulate and enable research, development, test, evaluation and timely transition of homeland security capabilities to Federal, state and local operational end-users.

In FY 2003 and FY 2004, the Rapid Prototyping portfolio provided funding of $30 million each year through our Homeland Security Advanced Research Projects Agency (HSARPA) to the interagency Technical Support Working Group (TSWG) to solicit ideas, concepts and technologies for 50 requirement areas of interest to both the Department and TWSG; initial contracts have been made and HSARPA will provide the programmatic monitoring of those efforts for the Science and Technology Directorate. This portfolio also provided support through HSARPA for a joint port and coastal surveillance prototype testbed designated "HAWKEYE" with the United States Coast Guard. Funding has been made available to support the creation of a Technology Clearinghouse as required in the Homeland Security Act of 2002.

In FY 2005, this program will continue to provide a mechanism for accelerated development of technologies relevant to homeland security in a process driven by technology developers. Through rapid prototyping and commercialization, these technologies will be made available to operational end-users as quickly as possible, thus increasing their capability to secure the homeland.

Support to Department of Homeland Security Components

As I have mentioned, the operational components of the Department are my customers. The Department of Homeland Security's Science and Technology Directorate supports the missions of the Information Analysis and Infrastructure Protection (IAIP) Directorate, Border and Transportation Security (BTS), Emergency Preparedness and Response (EP&R), United States Coast Guard (USCG), and United States Secret Service (USSS). Our TVTA portfolio supports the mission of the IAIP Directorate as previously indicated. This portfolio places high priorities on high-risk, high-reward research and development relevant to homeland security that might not otherwise be conducted in support of the missions of BTS, EP&R, USCG, and the USSS.

In FY 2003 and FY 2004, we continued to support the conventional missions of these operational components. Ongoing activities within BTS, USCG and USSS focus on

preventing terrorists and terrorist weapons (particularly weapons of mass destruction) from entering the United States, on detecting and preventing cyber attacks, supporting maritime transportation, safety and economy (Port and Channel navigation, Search and Rescue, and Aquatic Nuisance Species Remediation), and on preventing attacks on United States Secret Service protectees and high-visibility venues.

Support to Border and Transportation Security

The Science and Technology Directorate supports all elements of BTS enforcement and facilitation processes through identifying operational requirements, developing mission capabilities-based technological needs and implementing a strategic plan. We are providing systems engineering support to various BTS programs including US VISIT and Unmanned Aerial Vehicles.

The Science and Technology Directorate's support to the BTS Directorate is accomplished by implementing a capabilities-based technology planning process. The capabilities-based approach establishes the scope of effort and framework for a technology plan. Through a series of user conferences and technology opportunity conferences, requirements are developed and prioritized for new and improved capabilities. Operational personnel identify capabilities and technology personnel identify potential development opportunities. Capability gaps and possible technology solutions are proposed, and a budget is developed to distinguish between both funded and unfunded needs.

The Science & Technology Directorate co-chairs with BTS, the Department's Unmanned Aerial Vehicle (UAV) Working Group, which is currently focused on developing the Border and Transportation Security operational requirements for UAVs and related technologies, e.g., aerostats, blimps, lighter than air (LTA) ships, and fixed and mobile towers. The starting point for the requirements generation process is six BTS capability objectives we have identified that could benefit by the utilization of UAVs: surveillance and monitoring communications, apprehension, targeting, intelligence, deterrence, and officer safety. Functional capabilities that could be filled or improved through the application of UAVs and other technologies have been identified. Based on these high-level requirements, the Science and Technology Directorate is developing concepts of operations and assumptions that will be used in conducting an Analysis of Alternatives that will include UAVs and other technologies.

In FY 2005 we will be involved in a wide range of activities supporting the components, based upon their needs. For BTS, we will focus on discovering and implementing technologies that include improved screening and inspection, access control, document verification and validity, and data compression and analysis.

Support to Emergency Preparedness and Response

The nation has more than 750 regionally accredited community colleges. Community colleges train more than 80 percent of our country's first responders; these first

responders are critical for homeland security. The Science and Technology Directorate has a responsibility to ensure that these first responders have the necessary tools available to them to perform their jobs effectively and safely on a daily basis. This portfolio has a key role in our meeting that responsibility.

The scope of our EP&R portfolio includes research, development, test and evaluation for state, local and Federal emergency responders and emergency managers. Particular emphasis is placed on technology integration at all levels of government, technology insertion for weapons of mass destruction detection and monitoring systems, and long-term sustained performance and interoperability to enhance state and local preparedness.

Our work in the EP&R portfolio focuses on three major areas:

- Technology development for first responders
- Scientific and technical support to Federal response
- Technology integration – Safe Cities

The Safe Cities Program, a new initiative in FY 2004, is focused on implementing technology and operational system solutions in local communities/regions. This program is being piloted in a select number of cities in FY 2004 and will be conducted in close cooperation with state and local emergency managers and city planners to identify capability needs and gaps that advanced technologies being developed by the Science and Technology Directorate can meet. The Safe Cities Program seeks to provide technology and operational solutions that are sustainable by the communities in which they are implemented. The Safe Cities Program will enable us to better understand the operational context into which new technologies will be inserted. The Program will result in the creation of an infrastructure that facilitates the evaluation of new technologies in real-world operating environments as well as providing a venue for integrating these technologies with existing state and local systems.

In FY 2005 the EP&R portfolio will continue its focus on technology development and technical guidance for first responders (state and local), scientific and technical support to the EP&R Directorate; and expansion of technology integration — Safe Cities.

Support to United States Coast Guard

The Science & Technology Directorate is integrating a major research program into a United States Coast Guard operational testbed in south Florida. The HAWKEYE program injects technologies (such as Surveillance, Command & Control, Sensor Fusion, and Communications) allowing simultaneous evaluation of technology performance as a direct impact on mission execution.

Support to the United States Secret Service

We have coordinated with the United States Secret Service and established its first direct-funded R&D program. Based upon appropriated funding, four initiatives have been

identified and prioritized, and are underway in FY 2004. In addition, there will be joint activities in support of the assessment of emerging threats.

Homeland Security University and Fellowship Programs

In this portfolio we seek to develop a broad research capability within the nation's universities to address scientific and technological issues related to homeland security. The portfolio places high priorities on developing academic programs and supporting students in order to build learning and research environments in key areas of Departmental interest.

In FY 2004, this portfolio established the Department of Homeland Security's first University-based Center of Excellence, for Risk and Economic Analysis of Terrorism Events. The Center, based at the University of Southern California, will assess the level of risk associated with various terrorist scenarios, in particular the potential economic consequences. A request for proposals has been issued for the next two Centers of Excellence, which will focus on Foreign Animal and Zoonotic Disease Defense and Post-Harvest Food Protection and Defense.

Last fall, we awarded our 2003-2004 academic year DHS Scholarships and Fellowships, and welcomed our new Scholars and Fellows with a reception in Washington, DC. The solicitation for this program received nearly 2,500 applications for 100 Scholarships and Fellowships. Besides making immediate contributions to homeland security-related R&D, these students will be part of the development of a broad research capability within the Nation's universities to address scientific and technological issues related to homeland security.

During FY 2005, another 100 Scholars and Fellows will be supported for the academic year of 2004-2005, bringing the total of supported students to 200. We will also continue to support the Homeland Security University Centers of Excellence established in FY 2004, each with a different subject expertise focused on reducing the terrorist threat on the United States. Each Center of Excellence is awarded an initial three-year contract whose annual cost we account for in our planning.

Counter-MANPADS

The Counter-MANPADS program is focused on identifying, developing, and testing a cost-effective capability to protect the Nation's commercial aircraft against the threat of man-portable, anti-aircraft missiles. This program also provides the science and technology base needed to reduce the vulnerability of commercial aircraft to terrorist attack using man-portable anti-aircraft missiles.

Over the past year, we have had a successful solicitation announcing a program to address the potential threat of MANPADS to commercial aircraft. White papers responding to the Counter-MANPADS program solicitation were reviewed by technical experts from the Department of Homeland Security, Department of Defense, and other government agencies; proposals were evaluated; and awards were made to three

contractor teams to perform the first of two program phases, which began in January, 2004. The first phase will result in a preliminary design and a test plan to demonstrate missile countermeasure equipment on selected commercial aircraft.

The second program phase is an 18-month effort beginning in August 2004, with the one or two contractors that produced the most promising results in Phase One. During this phase, the commercial prototype countermeasure equipment will be integrated on selected commercial aircraft, and live-fire range tests will be accomplished with extensive data collection and analysis. Results of this second phase will be presented to the Administration and Congress to aid in formulating an informed decision on how best to address the protection of commercial airlines from the MANPADS threat.

SAFECOM

The SAFECOM (Wireless Public SAFEty Interoperable COMmunications) program is the umbrella initiative to coordinate Federal wireless investments and activities and partner with state, local, and Tribal governments to improve the interoperability of our nation's wireless communications. SAFECOM has three objectives: (1) Develop standards in partnership with Federal, state, local, and tribal public safety organizations to define the requirements for first responder interoperability at all levels; (2) Building from those standards, develop a national architecture in coordination with the work under the National Response Plan to assist in the progression towards wireless interoperability; and (3) Develop and implement a process to coordinate the Federal government's wireless interoperability investments and programs.

The placement of SAFECOM in the Department of Homeland Security's Science and Technology Directorate allows it full access to the scientific expertise and resources needed to help our nation achieve true public safety wireless communications interoperability.

The Science and Technology Directorate formally assumed responsibility for the management of Project SAFECOM in May 2003. Since then SAFECOM has:

- Developed and issued common grant guidance that was incorporated in the public safety wireless interoperability grant programs of both the Department of Justice and the Department of Homeland Security;

- Created for the first time, a Federal coordinating structure to coordinate all Federal public safety wireless interoperability programs; and

- Developed and published the first catalog of national programs touching on public safety wireless interoperability.

Our partnership with state, local, and tribal public safety organizations is critical to the future success of Project SAFECOM activities in standards development. To date, the results of our efforts reveal support from the community. The ten major state and local

organizations concerned with public safety wireless interoperability – the Association of Public-Safety Communications Officials (APCO), International Association of Fire Chiefs (IAFC), International Association of Chiefs of Police (IACP), Major Cities Chiefs Association (MCC), National Sheriffs' Association (NSA), Major County Sheriffs' Association (MCSA), National Association of Counties (NACO), National League of Cities (NLC), National Public Safety Telecommunications Council (NPSTC), and the United States Conference of Mayors (USCM) – released a statement in support of the SAFECOM program which declared that "With the advent of the SAFECOM Program . . . Public safety, state and local government finally have both a voice in public safety discussions at the Federal level and confidence that the Federal government is coordinating its resources."

Prioritization

The Science and Technology Directorate has prioritized its research and development efforts based on the directives, recommendations and suggestions from many sources, including:

- Homeland Security Act of 2002;
- The FY 2004 Congressional Appropriations for the Department of Homeland Security;
- President Bush's National Strategy for Homeland Security, the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, the National Strategy to Combat Weapons of Mass Destruction, the National Strategy to Secure Cyberspace, and the National Security Strategy;
- President Bush's nine Homeland Security Presidential Directives;
- Office of Management and Budget's 2003 Report on Combating Terrorism;
- Current threat assessments as understood by the Intelligence Community;
- Requirements identified by other Department components;
- Expert understanding of enemy capabilities that exist today or that can be expected to appear in the future; and
- The report from the National Academy of Science on "Making the Nation Safer: The Role of Science and Technology in Countering Terrorism," and the reports from the Gilmore, Bremer and Hart-Rudman Committees.

Identifying and integrating the information contained in these sources has not been a small task, but the result, coupled with expert evaluation and judgment by our scientific staff, is the basis for determining the research and development needed to meet our mission requirements.

Division of Effort Among the DHS S&T Directorate and Research Efforts at Other Government Agencies

One of the accomplishments of which I am personally most proud is the emphasis our new Directorate has put on interacting with other Federal departments and agencies. Knowledge of other science and technology programs and their results, appropriate

collaboration between agencies, coordination of relevant programmatic activities, and information sharing are essential for us to best meet our mission requirements. Science and Technology Directorate cybersecurity personnel and those at the National Science Foundation and the National Institute of Standards and Technology have already established collaborative and coordinated programs to ensure no duplication of effort. Additionally, we have incorporated an ongoing program managed by the Office of Law Enforcement Standards at NIST to develop a suite of personal protective and operational equipment standards for first responders. Inclusion of this multi-year program into our portfolio ensures that this effort can continue uninterrupted. Our biological and chemical countermeasures staff have partnered with the Department of Defense's (DOD's) Defense Threat Reduction Agency (DTRA) to plan and execute the BioNet program and roadmap the biological countermeasures R&D programs in both agencies to understand capabilities and shortfalls. They work with the National Science Foundation on pathogen sequencing. The BioWatch program, although led by the Science and Technology Directorate, was accomplished through collaboration with personnel from the Department of Energy's National Laboratories, contractors, the Environmental Protection Agency, and the Centers for Disease Control and Prevention. We work with DOD's Office of Homeland Defense to ensure the effective transfer to the Department of relevant DOD technologies. We work with the National Aeronautics and Space Administration as part of our efforts to assess the utility of aircraft and unmanned aerial vehicles to assist in border and coastal area control.

Our high explosives scientists are working with the interagency Technical Support Working Group, managed by the Department of State, to evaluate commercial off-the-shelf systems with capabilities against suicide bombers. The Director of the Homeland Security Advanced Research Projects Agency is a member of the TSWG Executive Committee. Our staff are in frequent contact with the Office of Science and Technology Policy on a range of issues, and several are members and co-chairs of the Office of Science and Technology Policy's National Science and Technology Council's Committees, Subcommittees and Working Groups. Our Office of Research and Development works closely with the Department of Agriculture to ensure that the Plum Island Animal Disease Center facility is operating smoothly and fully meeting its mission. The Office of Research and Development also interfaces with the Department of Energy to keep the Office of Science, as well as the National Nuclear Security Administration, apprised of our long-term homeland security requirements.

The Department of Homeland Security, Science and Technology Directorate recognizes that many organizations are contributing to the science and technology base needed to enhance the nation's capabilities to thwart terrorist acts and to fully support the conventional missions of the operational components of the Department. Congress recognized the importance of the research and development being conducted by numerous Federal departments and agencies, and, in the Homeland Security Act of 2002, directed the Under Secretary of Science and Technology to coordinate the Federal government's civilian efforts to identify and develop countermeasures to current and emerging threats.

We take this responsibility very seriously.

We are now initiating the effort needed to coordinate homeland security research and development across the entire United States Government. It will come as no surprise to the members of this Subcommittee that good, solid, effective research and development relevant to homeland security is being conducted by the Departments of Agriculture, Commerce, Defense, Energy, Justice, Health and Human Services, State, and Veteran's Affairs; within the National Science Foundation, the Environmental Protection Agency and other Federal agencies; and by members of the Intelligence Community.

Several interagency working groups already exist that are addressing issues important to homeland security. The Science and Technology Directorate has been, and continues to be, an active participant in these working groups, and in most cases has taken a leadership role. These fora foster an active exchange of information and assist each participating agency in identifying related needs and requirements, conducting research and development of mutual benefit, and avoiding duplication of effort.

We also continue to have discussions at multiple levels of management with Federal Departments and Agencies, as well as with the Office of Management and Budget, the Office of Science and Technology Policy, and the Homeland Security Council. These discussions ensure that the strongest possible links are made and the best possible coordination occurs between our Department and those who are conducting sector-specific research. By the autumn of 2004, all Department of Homeland Security research and development programs will be consolidated and all United States Government research and development relevant to fulfilling the Department's mission will have been identified and coordinated as appropriate. It is important to note that this identification and relevant coordination does not imply the Department of Homeland Security should have the responsibility and authority for these programs within other Federal agencies; it does recognize that science and technology advances can have many applications, including homeland security.

Outside Inputs to the S&T Budget

The Science and Technology Directorate's budget is built to meet the Department's and our mission requirements. As previously discussed, we identify and prioritize our efforts using multiple national sources and the sharing of information relevant to homeland security among government organizations. Our Homeland Security Science and Technology Advisory Committee will hold its first meeting February 26-27, 2004, and this group will also provide input to the scope, priority and level of effort needed to meet our objectives.

Metrics Developed by the Science and Technology Directorate

The success of the Science and Technology Directorate depends on its ability to identify, develop and transition capabilities to end-users that enhance the Nation's ability to protect itself. Appropriate goals and performance measures must be identified and used to

measure our progress. The following table identifies the programmatic metrics developed by the Science and Technology Directorate's portfolio managers; these metrics will be used to measure our performance.

ST0001 Biological Countermeasures

Long term performance goal	The United States will have a high-performance and well-integrated biological threat agent warning and characterization system that will include sustainable environmental monitoring capability for metropolitan areas; a national special security event system for the nation at large; and identification of needs for vaccines and therapeutics for people and animals. Longer term research will support the development of biological threat warning and characterization systems that address both current and future threats.

Performance Measures	**FY2005 Target**
Capability to detect and assess biological threats, measured by a set of attributes: increase sensitivity by decreasing false alarm rate (FAR), and increase multiplex samples.	FAR=10EE-4, Multiplex 10 assays
FY2005 milestones: Decontamination technologies and standards for facilities and outdoor areas. National Academy of Science study characterizes contamination risks.	Milestones will be achieved
FY2005 milestones: Establishment of a national capability in biodefense analysis and agro-bioterrorism countermeasures. Research operations begin; phased construction continues. BioForensics Analysis Center Hub operational.	Milestones will be achieved
Improved capabilities to detect threats in urban areas (Urban Monitoring Program), measured by increased sampling coverage and frequency, and capability to detect additional threats. FY2005 milestone: increase coverage in top threat cities.	Milestone will be achieved
Integrated field demonstrations of next-generation solutions (Domestic Demonstrations and Applications Program).	2 Demos operational
Validated human and agricultural bioassays.	10

ST0002 Chemical Countermeasures

Long term performance goal	Develop and deploy a broad capability to prevent and rapidly mitigate the consequences of chemical attacks.

Performance Measures	FY2005 Target
FY2005 milestone: Development of protocols for the highest priority toxic industrial chemicals (TICs) and toxic industrial materials (TIMs).	Milestone will be achieved

ST0003 Chemical High Explosives

Long term performance goal	The Chemical High Explosives portfolio will improve explosives detection equipment and procedures for all forms of transportation as well as fixed facilities.

Performance Measures	FY2005 Target
FY2005 milestone: Pilot tests of standoff detection technologies.	Milestone will be achieved

ST0004 Radiological & Nuclear Countermeasures

Long term performance goal	By FY2009, an effective suite of countermeasures against radiological and nuclear threats will be developed with capabilities in detection, intelligence analysis, response, and preparedness.

Performance Measures	FY2005 Target
Federal, state and local sites that are integrated into an operational secondary reachback architecture to resolve radiological and nuclear alarms.	5
Performance measures associated with Test and Evaluation (T and E) of developmental prototypes of Radiation Detectors. Establish a long-range plan for T and E capability.	Milestone will be achieved
Progression on planned capability development for Nuclear Incident Management and Recovery. Demonstrate 2 advanced detection technologies.	Milestone will be achieved

Progression on pre-planned product improvement of deployed technologies. Perform critical design reviews for Phase One technology improvements for projects awarded in FY2004.	Milestone will be achieved

ST0005 Threat and Vulnerability, Testing & Assessments

Long term performance goal	Provide measurable advancements in information assurance, threat detection and discovery, linkages of threats to vulnerabilities, and capability assessments and information analysis required by Departmental missions to anticipate, detect, deter, avoid, mitigate and respond to threats to our homeland security.

Performance Measures	FY2005 Target
Improvement in the national capability to assess threats and vulnerabilities to terrorist attacks: 10 categories to be assessed.	Improvement in 7 categories

ST0006 Standards

Long term performance goal	Establish an integrated infrastructure for determining and developing standards, and test and evaluation protocols for technology used for detecting, mitigating, and recovering from terrorist attacks and also to support other Departmental components' technologies. Provide consistent and verifiable measures of effectiveness of homeland security-related technologies, operators, and systems in terms of basic functionality, interoperability, efficiency, and sustainability. Facilitate the development of guidelines in conjunction with both users and developers.

Performance Measures	FY2005 Target
Long-term implementation of SAFETY Act	Certifications
FY2005 milestones: Technical standards and test/evaluation protocols will be established for Powered Air Purifying Respirators, WMD decontamination technologies and analysis tools. "Consumer's report" on radiation and bioagent detection devices for federal, state, and local users will be published. Continued certification testing of CBRN Self-Contained Breathing Apparatus, Air Purifying Respirators and Escape Masks.	Milestones will be achieved

ST0008 Homeland Security Fellowship Programs / University Programs

Long term	Significantly increase the number of U.S. students in fields

performance goal	relevant to homeland security including the physical life and social sciences; and engineering.

Performance Measures	FY2005 Target
To increase the nation's science and technology workforce and research capability on issues related to homeland security. FY 2005: students supported/Centers of Excellence established.	200 students 3 centers

ST0009 Emerging Threats

Long term performance goal	To develop effective capabilities to characterize, assess, and counter new and emerging threats, and to exploit technology development opportunities as they arise.

Performance Measures	FY2005 Target
Improved capability to prevent terrorist attacks through annual emerging threat assessment report (% of responding recipients indicating the report is valuable).	Baseline

ST0010 Rapid Prototyping

Long term performance goal	Support the development of innovative solutions to enhance homeland security and work with federal, state, and local governments; and the private sector to implement these solutions. In partnership with the Technical Support Working Group (TSWG), operate an effective and efficient clearinghouse that will develop, prototype, and commercialize innovative technologies to support the homeland security mission.

Performance Measures	FY2005 Target
Technologies prototyped or commercialized.	3

ST0011 SAFECOM

Long term performance goal	Improve interoperability of wireless communications among and between all levels of government through the development of standards, a national architecture and coordination of Federal programs and grants.

Performance Measures	FY2005 Target
Increased interoperability across local, tribal, state, and federal public safety jurisdictions and disciplines. FY 2005: Based on FY	3

2004 baseline, improvements in 3 categories.	

ST0012 Counter Man-Portable Air Defense System (MANPADS)

Long term performance goal	The Nation will have effective capabilities to defeat the threat to commercial aircraft of man-portable anti-aircraft missiles.

Performance Measures	**FY2005 Target**
Effective technology/technologies for commercial aircraft to defeat man-portable anti-aircraft missiles identified. FY 2005: Technologies identified, and prototypes developed and tested.	2

ST007 Support to Department of Homeland Security Components

Long term performance goal	Increase the capabilities of mission-focused operational components (BTS, EP&R, Coast Guard, and Secret Service) to secure the homeland and enhance their ability to conduct their missions.

Performance Measures	**FY2005 Target**
Improved capability of DHS Components to secure the homeland as measured by assessment of customer organizations in accomplishing agreed-upon areas of assistance.	Baseline

Short-Term and Long-Term Research.

In the approximately 13 months that this Department has been in existence, the Science and Technology Directorate has focused its initial efforts on near-term development and deployment of technologies to improve our nation's ability to detect and respond to potential terrorist acts. However, we recognize that a sustained effort to continually add to our knowledge base and our resource base is necessary for future developments. Thus, we have invested a portion of our resources, including our university programs, toward these objectives. The following table indicates our expenditures in basic research, applied research, and development to date, excluding construction funding.

Science and Technology Directorate R&D Investments (in millions of $)			
Fiscal Year	**FY 2003(actual)**	**FY 2004(estimated)**	**FY 2005(proposed)**
Basic	47	117	80
Applied	59	56	229
Developmental	398	608	643
Total	**504**	**781**	**952**
% basic	**9.3%**	**15.0%**	**8.4%**

Our initial expenditures in basic research are heavily weighted by our investments in university programs. These university programs will not only provide new information relevant to homeland security, but will also provide a workforce of people who are cognizant of the needs of homeland security, especially in areas of risk analysis, animal-related agro-terrorism, bioforensics, cybersecurity, disaster modeling, and psychological and behavioral analysis.

We expect to gradually increase our total percentage of basic and applied research to the level needed for sustaining our role as a research, development, testing and evaluation (RDT&E) organization.

Rationale for Budget Increases: BioWatch and the National Biodefense Analysis and Countermeasures Center

President Bush's Fiscal Year 2005 budget request includes a $274 million Bio-Surveillance Program Initiative to protect the nation against bioterrorism and to strengthen the public health infrastructure. Included in this request is an increase of $65 million for the Science and Technology Directorate to enhance current environmental monitoring activities. This requested increase is a direct outgrowth of the recently completed joint Homeland Security Council – National Security Council (HSC-NSC) Bio-Defense End-to-End study which identified the need for an integrated, real-time, human-animal-plant surveillance system as a top priority national need. The DHS BioWatch system, which currently provides a bio-aerosol warning for most of this nation's large metropolitan areas, figures prominently in the integrated Biosurveillance initiative. This initiative would entail: (1) Expanding BioWatch coverage in the top ten threat cities; and (2) Piloting of an integrated attack warning and assessment system known as BWICS (BioWarning and Incident Characterization System). Currently the "average" BioWatch city has about 10 collectors per city. Systems studies and city feedback provide a more 'needs based' guide to the optimal number of collectors in our large, high threat cities. The systems studies show that about 40-60 collectors provide optimal outdoor coverage for a city, while the cities themselves have requested additional collectors for key facilities (transit systems, airports, stadiums). Alternate labor

contracting processes, simplified sample handling techniques, and the introduction of additional automation in analyses will allow us to do this expansion in a cost effective manner.

The BWICS pilot will integrate real-time bio-surveillance and environmental monitoring data with plume hazard predictions, epidemiological forecasts, population and critical infrastructure databases, and other available resources in two of the highest threat cities.

We also will accelerate R&D on next generation environmental monitoring systems. New classes of detectors, that can identify bio-agents in two minutes or less with incredibly low false alarm rates will make it possible to do 'detect-to-protect' for key facilities – allowing one to reroute air flow or evacuate a facility so as to minimize exposure and not simply begin the onset of early treatment. And tailoring of existing and emerging detection systems to monitoring key high volume nodes in our food processing will be critical to the development of proposed 'food shields.'

The National Biodefense Analysis and Countermeasures Center (NBACC) provides scientific support for intelligence activities, prioritizes biothreats, and also conducts bioforensic analyses contributing to attribution and hence to deterrence. Specifically, the NBACC (both facilities and programs) will support public and agricultural health, law enforcement, and national and homeland security by providing hub laboratory capabilities for:

- Dedicated and accredited bio-forensic analysis capabilities to support attribution of the use of bio-threat agents (BTA) by criminals, non-state, and state-sponsored actors
- Laboratory-based, scientific data from the analysis and assessment of biological threats to human health and agriculture to support a national bio-defense net assessment – fundamental to development of national plans, risk assessment evaluations and priorities to deter, detect, mitigate and recover from BTA attack
- Applied models, materials, and validation processes to evaluate BTA countermeasures
- Evidenced-based subject matter expertise to integrate, analyze and distribute critical bio-defense and related information assembled from multiple sources through a high security and open clearinghouse.

Transfer of R&D Budgets and Activities from Other Directorates

The Science and Technology Directorate is both a generator and a consumer of scientific and technological advances resulting from basic and applied research and development. We also have a responsibility for testing and evaluating capabilities to ensure that their deployment results in improved operational systems. Standards are needed to assist first responders and operational components of the Department in evaluating, procuring, and deploying new capabilities. This is a broad range of responsibility and one we take seriously. The Department has defined R&D activities as follows:

> Activities associated with R&D efforts include the development of a new or improved capability to the point where it is appropriate for operational use, including test and evaluation. R&D activities include the analytic application of scientific and engineering principles in support of operational capabilities, concept exploration, systems development, proof of principle demonstration and pilot deployments, standards development, and product improvement including application and integration of technologies. For mission (non-management) systems, resources associated with developing technology to provide new capabilities (including systems engineering, research, development, testing and prototyping) are covered under the R&D category.

This definition encompasses all of the research, development, test, and evaluation (RDT&E) efforts of the Science and Technology Directorate. It also encompasses RDT&E efforts currently existing in other parts of the Department of Homeland Security. The Science and Technology Directorate has been tasked to consolidate these activities from elsewhere within the Department into our directorate.

We have begun this coordination process by evaluating and producing a report on the research, development, testing, and evaluation work that was being conducted within the Department of Homeland Security but was not already under the direct cognizance of the Science and Technology Directorate. Where it is appropriate, the Science and Technology Directorate will absorb these R&D functions. In other cases, the Science and Technology Directorate will provide appropriate input, guidance, and oversight of these R&D programs.

Research and Development activities are ongoing in FY 2004 within the following departmental elements: Border and Transportation Security (BTS), Emergency Preparedness and Response (EPR), United States Coast Guard (USCG), and United States Secret Service (USSS). The Information Analysis and Infrastructure Protection (IAIP) Directorate reported no FY 2004 R&D activities.

The FY 2005 President's Budget contains three programs that have been identified to transfer to the Science and Technology Directorate. They are United States Coast Guard RDT&E activities conducted at their Groton, CT laboratory; Emergency Preparedness and Response RDT&E activities supporting the U.S. Fire Administration; and ICE-Federal Air Marshall's RDT&E activities supporting the development of their Air-to-Ground Communication System.

The transfer of these three RDT &E Programs is only the start and not the complete identification of the potential programs to review for consideration. S&T will be working throughout the year with the Department and with Congress to identify other existing programs and transfer them consistent with direction.

Budget and Activities Supporting Cybersecurity R&D

The cybersecurity program within the Science and Technology Directorate is conducted by the Threat and Vulnerability, Testing and Assessment portfolio. The approach of this program includes addressing areas not currently addressed elsewhere in the Federal government. An example of this is developing tools and techniques for assessing and detecting the insider threat. The cybersecurity budget request for FY 2005 is $18 million dollars.

An important component of the cybersecurity program is coordination with others who are performing cyber research and who are responsible for cybersecurity. For example, our syaff have engaged in a series of meetings with staff members from the Department's Information Analysis and Infrastructure Protection Directorate (IAIP), both the National Cyber Security Division and National Communications System. These meetings provide an venue for general exchanges of information about each organizations' respective plans for cybersecurity, as well as specific discussions focused on IAIP technical requirements to feed into cybersecurity R&D programs funded by the Science and Technology Directorate.

Further, we are coordinating with the National Institute for Standards and Technology (NIST) and the National Science Foundation (NSF) to plan our respective roles. We are funding two projects with NIST, Secure Domain Name System and Secure Border Gateway Protocol, which are protocols that the Internet relies on to function. We are co-funding two projects with the NSF: a research project to create an experimental infrastructure network to support development and demonstration of next generation information security technologies for cyber defense, called Cyber Defense Technology Experimental Research ("DETER") Network; and a project called Evaluation Methods in Internet Security Technology (EMIST), a testing framework that will include attack scenarios, attack simulators, generators for topology and background traffic, data sets derived from live traffic, and tools to monitor and summarize results.

Basis for Policy on the Use of the National Laboratories

The research, development, testing, and evaluation capabilities needed to support the missions of the Department of Homeland Security are being defined and institutionalized within the Department. Support of those needs now and in the future requires the establishment and support of an enduring capability that includes scientists and engineers who are well-versed in the requirements and technologies associated with homeland security, and dedicated to the mission of the Department, as well as physical facilities that support their efforts. The legislation creating the Department of Homeland Security and the Science and Technology Directorate recognized that many of these needed capabilities exist within the Department of Energy's (DOE's) laboratories and sites and provided for access to them in support of the Department's mission.

The DOE laboratories have sufficient critical mass and expertise across multiple disciplines to perform the necessary threat assessments and, thus, to participate in DHS's

and the S&T Directorate's internal systems analyses, associated trade studies, and long-range planning that will form the basis for the architectures that are ultimately developed and deployed to secure the homeland. These scientists will be intimately involved in assisting the S&T Directorate in setting research goals and requirements and formulating the research and development roadmaps.

A number of approaches have been explored to enable the most effective and appropriate use of these vital resources. Current law, regulation, and policy allows the DOE laboratories to respond as prime contractors, subcontractors or team members to open general research or technical assistance requests to the private sector, such as Broad Agency Announcements (BAAs) or similar solicitations. However, the S&T Directorate has always recognized the critical importance of ensuring a "level playing field", and hence the need for guarding against organizational conflicts of interest and inappropriate use of "inside information" for those organizations responding to open solicitations to the private sector. The first mechanism that the S&T Directorate explored to address this concern was the concept of "intramural" and "extramural" laboratories. In this approach, some DOE laboratories would be considered part of the intramural team for planning purpose, and others would be considered extramural. Only extramural labs would be eligible to respond to HSARPA and SE&D solicitations. This approach has now been revisited based on the direct feedback from several of the laboratories. However, the need to ensure equity in the process and preclude organizational conflicts of interest remains.

Laboratories that have access to government planning information – and thus in fact are part of the planning process – will not be able to participate in BAAs or similar solicitations issued by DHS. These funding sources currently represent the majority of the funding that the S&T Directorate will spend on developing technologies for DHS. All of the DOE laboratories will be eligible for project funding from S&T's Office of Research and Development, however. In addition, those laboratories that do not contribute to our planning would be able, as the law permits today, to respond to BAAs or similar solicitations issued by DHS. The decision as to whether a laboratory wants to be positioned to potentially participate in our planning processes, and hence to be ineligible for DHS funding made available through BAAs or similar solicitations, will be a decision each laboratory will make individually.

Budget for University Centers of Excellence and Fellows Programs

The President's FY05 budget request of $30 million will sustain the current scholars and fellows program and a total of three Homeland Security Centers of Excellence. Each additional Center of Excellence would require a sustained investment of $5 million per year.

Staffing

When the Department of Homeland Security (DHS) stood up on March 1, 2003, the Science and Technology Directorate had a total staff of about 87, including the 53 staff transferred from the Department of Energy's Environmental Measurements Laboratory. The balance was comprised of permanently assigned personnel, employees detailed from within and without the Department, Intergovernmental Personnel Act assignments, and personnel support from the National Laboratories.

By January 6, 2004, we more than doubled our staff. In January 2004, we had a total staff of 212, including 100 DHS employees, six Public Health Service Officers, 21 Intergovernmental Personnel Act employees, 26 individuals on assignment from other agencies, and 59 contractors.

We continue to be active in staffing our Directorate with well-qualified individuals whose skills support the full breadth of our responsibilities and RDT&E activities. We continue to actively seek additional staff in accordance with our approved staffing plan.

Conclusion

With just over a full year under the Department's belt, the scientists and engineers in the Science and Technology Directorate have accomplished more than I could have expected. I am proud to have shared with you today some of those success stories. We have appended a more comprehensive summary of accomplishments to date for the record.

And yet, we also recognize that there is much to do, and we will be working just as hard in FY 2005.

I look forward to continuing to work with you on the House of Representatives Appropriations Subcommittee on Homeland Security; other Federal departments and agencies; the academic community; and private industry to continue the work begun and continually improve our ability to protect our homeland and way of life.

Mr. Chairman, Congressman Sabo, and Members of the Subcommittee, this concludes my prepared statement. I thank you for the opportunity to appear before this committee and I will be happy to answer any questions you may have.

Appendix

Accomplishments of the Science and Technology Directorate

Department of Homeland Security

March 2003 to February 2004

Biological and Chemical Countermeasures

Biowatch: National Urban Monitoring for Biological Pathogens

The Biowatch program has been established and deployed to cities across the nation. The program – developed, funded, and managed by the Science and Technology (S&T) Directorate – is executed in cooperation with the Environmental Protection Agency (EPA) and the Centers for Disease Control and Prevention (CDC). It employs environmental sampling devices to quickly detect biological pathogens, such as anthrax, in time to distribute life-saving pharmaceuticals to affected citizens. The S&T Directorate is now focusing its efforts on piloting the next generation of environmental samplers, which will reduce the amount of labor required and the response time needed for detection while keeping the detection probability high and false alarm rates low. These devices will take advantage of the latest advances in micro-chemistry, commonly referred to as "chemistry on a chip."

PROTECT (Program for Response Options and Technology Enhancements for Chemical Terrorism): Chemical Defense and Response Capability for Transportation Facility

The S&T Directorate, in collaboration with the Washington Metropolitan Area Transit Authority (WMATA), completed PROTECT (Program for Response Options and Technology Enhancements for Chemical/Biological Terrorism). PROTECT, which is an operational chemical agent detection and response capability, is deployed in Metro stations and operated by the WMATA. PROTECT is a team effort that owes its success to the scientific and engineering talent from Argonne, Sandia, and Livermore National Laboratories and operational expertise from WMATA and the First Responder community (the District of Columbia; Arlington, VA; Montgomery County, MD; and others). Also contributing significantly to the project are private industry partners, including LiveWave Inc., ManTech Security Technology, the detector manufacturer (name withheld for security reasons); and Federal partners, including the Federal Transit Administration (FTA), Department of Transportation (DOT), National Institute of Justice (NIJ), and the Department of Homeland Security's (DHS's) Office of Domestic

Preparedness (ODP). The system integrates chemical detector data and video feed and transmits the integrated information to the Operation Control Center (OCC), where the information is analyzed and an event confirmed. The information is then transmitted to the first responders who access it in both their OCC and through the use of wired jacks on the scene to facilitate response and recovery. PROTECT also has application in other areas, including fire and emergency response, security, and forensics. Upon completion, the system will be totally owned and operated by WMATA and expanded to approximately 20 stations. FTA is working with WMATA and Argonne National Laboratory to transfer the technology nationally. The information gleaned from PROTECT will have direct application to facility protection and response. A related effort is being piloted in the Boston subway system.

Joint Urban 2003**:** Experimental Atmospheric Transport and Modeling

In June 2003, the S&T Directorate, in coordination with the Department of Defense's Defense Threat Reduction Agency, Department of Energy, and University of Oklahoma sponsored a month-long atmospheric dispersion study in Oklahoma City, OK. Nearly 150 scientists, engineers, and student assistants were dedicated to this study, which tracked the air movement of safe, non-toxic tracer gases in and around city buildings. The resulting data is being used to enhance and develop urban-specific atmospheric dispersion computer models that will allow emergency management, law enforcement and other personnel to train for and respond to potential chemical, biological, and radiological terrorist attacks.

ProACT (Protective and Response Options for Airport Counter Terrorism): Chemical and Biological Counterterrorism Demonstration and Application Program

The S&T Directorate and its partners at the San Francisco International Airport are involved in a pilot program that couples biological and chemical detection with vulnerability analysis, response, and restoration. This program integrates networked sensors with the operation of ventilation systems, allowing redirection of contaminated air and effective evacuation should an event occur. Guidance for the airport facility operators to manage biological and chemical crises will be finalized soon for distribution throughout the applicable community. Protocols and concepts of operation for restoration also are under development. This program is designed to serve as a template for deployment of these capabilities to other similar facilities.

LINC (Local Integration of National Atmospheric Release Advisory Center [NARAC] with Cities): Hazard Assessment Tool for Operational Event Management

LINC demonstrates the capability for providing local government agencies with advanced operational atmospheric plume prediction capabilities that can be seamlessly integrated with appropriate federal agency support for homeland security. LINC's approach is to integrate NARAC capabilities with local emergency management and response centers. In the event of a chemical or biological release, NARAC predictions can be used by emergency managers and responders to map the extent and effects of

hazardous airborne material. Prompt predictions are provided to guide front-line responders in determining protective actions to be taken, critical facilities that may be at risk, and safe locations for incident command posts. LINC provides response teams from multiple jurisdictions with tools to effectively share information regarding the areas and populations at risk. To date, several cities have participated in the project. New York City used LINC to help inform and manage an explosion and fire at a Staten Island refinery in the Spring of 2003.

BioNet: Integrated Civilian and Military Consequence Management

The Department of Homeland Security (DHS) and the Department of Defense's Defense Threat Reduction Agency have initiated the BioNet program to address joint civilian-military consequence management issues for localities near military bases. Upon completion of BioNet, a seamless consequence management plan that incorporates concepts of operation, information products, area monitoring, population health monitoring, and sample analysis laboratory will be developed that can be used nationally.

Plum Island Animal Disease Center (PIADC)

The S&T Directorate assumed responsibility for the operations of the "facilities and liabilities" of PIADC in June 2003. A 60-day review of security and operations resulted in immediate improvements and a plan for enhancements to security and operational maintenance. Dr. Beth Lautner has become new Center Director for PIADC. Dr. Lautner was with the National Pork Board for 13 years, most recently serving as the vice-president of Science and Technology. Highly respected throughout animal agriculture for her work on numerous issues, she pioneered the establishment of the Pork Quality Assurance (PQA) Program and has worked extensively with the USDA and other organizations on national agricultural security issues. In 1994, she was awarded the prestigious Howard Dunne Memorial Award by the association. In addition, DHS announced on December 9, 2003, the selection of Field Support Services, Inc. (FSSI), as the new contractor for maintenance at PIADC. FSSI is a subsidiary of Arctic Slope Regional Corporation, an Alaskan Native corporation, headquartered in Barrow, Alaska.

TOPOFF2 Exercise

In May 2003, leadership and staff members of the Science and Technology Directorate served as members of the Secretary's Crisis Assessment Team (CAT) and the interagency Domestic Emergency Support Team (DEST) and provided expert technical advice on understanding, communicating and responding to the hypothetical radiological and plague events during the TOPOFF2 exercise.

Radiological and Nuclear Countermeasures Programs

Radiation Detection in Metropolitan Areas

The Science and Technology division formally assumed management of the Port Authority of New York and New Jersey's radiation detection test bed on August 2003. The test bed was previously managed by the U.S. Department of Energy. The transfer will broaden the project scope beyond testing and evaluation of individual pieces of technology to a systems approach including response protocols and operational concepts. Radiation detection equipment will be installed at tunnels, bridges, ports, and airports in the New York City metropolitan area, and all functions associated with their operational use will be evaluated. By judging the efficacy of fielded systems over time, the Science and Technology division will be able to influence future decisions on detection technology R&D investment, deployment of urban monitoring systems, configurations best able to enhance security, and viable solutions for protecting the nation from radiological and nuclear threats.

Determined Promise Exercise

In August 2003, staff members of the S&T Directorate participated in Determined Promise, a Department of Defense (DoD) exercise held in Las Vegas, NV. The exercise demonstrated the military's capability to assist in the response to a natural disaster, a bioterrorism event, and a number of other emergency situations nationwide. The exercise also provided a forum for initiating discussions that will foster interagency cooperation between DHS and USNORTHCOM.

Nuclear Threat Assessments

The S&T Directorate has provided eight rapid nuclear threat assessments for the Federal Bureau of Investigation (FBI), and approximately two dozen assessments on reports of illicit trafficking in nuclear materials for the Department of State and other customers. The Department of Homeland Security has been leading the interagency Nuclear Trafficking Focus Group, which regularly brings together the operational players of all agencies involved in response to and understanding of nuclear smuggling events.

Secondary "Reach Back"

In August 2003, the S&T Directorate's Nuclear Assessment Program stood up a system to provide secondary "reach back" support to operational DHS entities employing radiation detection systems in the field. Secondary reach back provides inspectors with an additional information resource to utilize for the resolution of radiation detection alarms that draws upon experience in the analysis of nuclear smuggling incidents and threat analysis.

Standards

Radiation Detection.

The S&T Directorate has developed a suite of four radiation detector standards under the auspices of the American National Standards Institute (ANSI)'s Accredited American Standards Committee on Radiation Instrumentation. The four standards deal with radiation pagers, hand-held dosimetry instruments, radioisotope identifiers and radiation portal monitors. The S&T Directorate has formed three writing groups to prepare Test and Evaluation (T&E) protocols for hand-held radiation detectors, radionuclide identifiers and radiation portal monitors. The writing groups have met in working sessions in San Diego, CA (July 2003) and Las Vegas, NV (September 2003) and have prepared draft T&E protocols. Benchmark testing against these draft protocols has been initiated at four National Laboratories.

Biopathogen Identification

The Science and Technology Directorate has partnered with the Department of Defense, Office of the Secretary of Defense to fund a contract with the Association of Analytical Communities International to develop Reference Methods and Official Methods for bulk assay of *bacillus anthracis*. This work will also permit the comparison of commercially available rapid identification methods (hand-held assays) for *B. anthracis*.

Personal Protective and Operational Equipment Standards

The S&T Directorate in 2004 incorporated the First Responder CBRN Personal Protective and Operational Equipment Standards Development Program into its standards portfolio. This multi-year program, executed through the Office of Law Enforcement Standards at NIST; develops equipment performance standards, test methods, conformity assessment programs, user guides to meet first responder needs for CBRNE incidents. S&T adopted three CBRN respiratory protection standards developed by the National Institute for Occupational Safety and Health (NIOSH) developed through this program and five standards from the National Fire Protection Association (NFPA) in February.

SAFETY Act

On October 10, 2003, Secretary Ridge signed an interim final rule implementing the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act which was a requirement of the Homeland Security Act of 2002. The SAFETY Act is designed to encourage the development and rapid deployment of life-saving, anti-terrorism technologies by providing manufacturers and sellers with limited liability risks. The Department is now accepting applications for designation under the Act and evaluating the proposed technologies.

Interoperability of Communications

SAFECOM: E-Gov Initiative to Improve Interoperability of Wireless Communications

The Department of Homeland Security is taking steps to boost the ability of the approximately 44,000 local, tribal and State entities and 100 federal agencies engaged in public safety to communicate effectively with one another, particularly during an emergency. SAFECOM is a Federal umbrella program under the S&T Directorate that is dedicated to improving public safety response through the development of standards and a national architecture that will promote enhanced interoperable wireless communications. The goal is to enable public safety agencies to talk across disciplines and jurisdictions via radio communications systems, exchanging voice or data with one another on demand and in real time. SAFECOM also partners with the joint Department of Justice and Department of Homeland Security Integrated Wireless Network program, which will create interoperability among local, state and federal public safety agencies in 25 cities. In addition, technical guidance for interoperable communications that was developed under SAFECOM is included in this year's Office of Domestic Preparedness grants.

Summit on Interoperable Communications for Public Safety

In June 2003, the S&T Directorate, Project SAFECOM, the National Institute of Standards and Technology (NIST) and the National Institute of Justice hosted a Summit on Interoperable Communications for Public Safety. The event focused on familiarizing attendees with programs that assist public safety practitioners, including first responders, and is the first national effort ever undertaken to convene all the players. In addition, it provided insight on how government can leverage existing program successes and resources in the area of standards development, approaches, and products and services. The Summit results provided help in formulating a coordinated approach toward nationwide communications interoperability.

SAFECOM Vendor Demonstration Day

In August 2003, the Science and Technology Directorate held its first SAFECOM Vendor Demonstration Day, with an overwhelmingly positive response from technology providers. Due to the increasing number of vendor requests to present their technologies to the SAFECOM Program, the S&T Directorate is holding a vendor demonstration day on the last Friday of every month. These Friday sessions will offer a chance for SAFECOM to learn about new technologies for interoperability, provide a clear process for managing vendor requests, and provide an opportunity for vendors to participate.

SAFECOM held a Vendor Demonstration Day on January 30, 2004. SAFECOM's Vendor Day allows several communications equipment and service providers to present their products and/or technologies for SAFECOM. Responses from the SAFECOM Request for Information in November 2003 were used to select vendors for this event.

Each vendor selected represents a different approach to solving the communications and interoperability problems facing first responders.

Information Analysis and Infrastructure Protection Programs

Addressing Threats and Vulnerabilities in the Oil and Gas Industries

The S&T Directorate sponsored and delivered a prototype system to the Information Analysis and Infrastructure Protection (IAIP) Directorate to perform Graphical Information System (GIS) based computer assisted threat and vulnerability mapping of the oil and gas infrastructure in the American Southwest. S&T is also in the process of delivering to IAIP cutting edge visualization, data searching, data correlation, and all-source analytic aids to provide IAIP advanced analytic capabilities integrated with vulnerability information.

Advanced Algorithms for Biodetectors

Researchers funded by the S&T Directorate's Advanced Scientific Computing Research & Development program achieved an important milestone in the speed acceleration of software used to develop advanced biodetectors. Scientists have made a pair of related algorithmic advances that will speed the creation of DNA signatures for pathogen detection at considerably reduced cost. These discoveries will result in cheaper, faster, and more reliable bio-detectors for homeland security.

Threat-Vulnerability Mapper

Part of the Threat-Vulnerability Information System, the Threat-Vulnerability Mapper (or TVM), was installed in the analysis center of the Information Analysis and Infrastructure Protection Directorate in December 2003 and is already in constant use. Developed by the S&T Directorate, the TVM provides counterterrorism analysts with a simple, straightforward way to not only depict the geographic distribution of threats across the United States, but also to search the underlying databases for information on the possible actors, agents, potential severity of attacks, and extent of the vulnerabilities to and effects of such attacks. A second TVIS component was delivered to IAIP in January 2003 and should be installed and operational by the end of February 2004.

Critical Infrastructure Protection Decision Support System

On December 24, 2003, S&T's Critical Infrastructure Protection Decision Support System (CIP/DSS) team was asked to conduct a rapid analysis of potential consequences following discovery of a cow in Washington State with bovine spongiform encephalopathy (BSE), commonly known as Mad Cow disease. An analysis was developed within hours using available open literature, past historical data, and the results from an early stage, Dynamic Simulation agriculture model.

Cybersecurity

Experimental Infrastructure Network for Cyber Defense

Led by the S&T Directorate, DHS is co-funding with the National Science Foundation a $5.45M, three-year research project to create an experimental infrastructure network to support development and demonstration of next generation information security technologies for cyber defense. This project supports national-scale experimentation on emerging security research and advanced development technologies. Called Cyber Defense Technology Experimental Research ("DETER") Network, this is a multi-university project led by the University of California, Berkley.

Evaluation Methods in Internet Security Technology

DHS is co-funding with the National Science Foundation, a second cyber security project called Evaluation Methods in Internet Security Technology (EMIST). EMIST is a testing framework that can be adapted to simulators, emulation facilities, other testbeds, and hardware testing facilities. The framework will include attack scenarios, attack simulators, generators for topology and background traffic, data sets derived from live traffic, and tools to monitor and summarize results. EMSIT is a three-year, $5.6M, multi-university research project that includes Penn State; University of California, Davis; Purdue; and the International Computer Science Institute.

United States Coast Guard

Maritime Surveillance Testbed Prototype

In September 2003, S&T's Homeland Security Advanced Research Projects Agency and the United States Coast Guard planned and funded the South Florida Coastal Surveillance Prototype Testbed, a port and coastal surveillance prototype in Port Everglades, Miami, and Key West areas. The prototype is an evolutionary testbed that:

- Provides an initial immediate coastal surveillance capability in a high priority area
- Offers the Coast Guard and other DHS agencies the means to develop and evaluate CONOPS (Concept of Operations) in a real world environment
- Implements and tests interoperability among DHS and DoD systems and networks such as the US Navy/Coast Guard Joint Harbor Operations Center (JHOC).
- Tests and evaluates systems and operational procedures
- Becomes the design standard for follow-on systems in other areas and integration with wider area surveillance systems.

The program has two phases; an initial prototype development phase, and an improvements and update phase. The program is expected to begin operations in June 2004 and is funded at $2.4M for FY 2003 and $5M for FY 2004 .

Partnerships

Workshop on Scientific Computing in Support of Homeland Security

The Science and Technology Directorate brought together experts from academia, private industry and the national laboratories with staff from various organizations within the Department to understand how the S&T Directorate's advanced scientific computing (ASC) capabilities, centered at the national laboratories, can help address needs across the Department. This workshop, held October 8-9, 2003, has resulted in identifying several areas of potential high payoff for the use of these unique capabilities; two examples are advanced research in data management and information extraction, and research and development of computational simulation tools. The workshop will produce a formal report identifying relevant ASC capabilities and matching them up with identified needs within the Department of Homeland Security for improved operational capabilities.

Infrastructure Subcommittee of the National Science and Technology Council

Staff members of the Science and Technology Directorate had a major role in drafting the first charter for the National Science and Technology Council's (NSTC's) Infrastructure Subcommittee; the Subcommittee's first Co-Chairs are from the S&T Directorate and the Office of Science and Technology Policy. The Subcommittee serves as a forum within the National Science and Technology Council (NSTC) for developing consensus and resolving issues associated with coordinating R&D agendas, policy, and programs to develop and protect the nation's infrastructure. The Subcommittee will also be the vehicle used by the Department of Homeland Security and the White House Office of Science and Technology Policy to develop the National R&D Plan for Critical Infrastructure Protection.

Homeland Security Standards Panel

The S&T Directorate worked with the American National Standards Institute (ANSI) and the National Institute of Standards and Technology (NIST) to establish a Homeland Security Standards Panel (HSSP) that would coordinate the development of consensus standards among the 280 different standards development organizations. On June 9-10, 2003, the inaugural meeting of the ANSI Homeland Security Standards Panel was held at NIST. Plenary session presentations were given by four S&T Directorate staff members to outline the needs in Department for standards. The panel selected a small list of topics to address with focus workshops. The first of these occurred in September 2003 with a focus on needs for standards in biometrics.

Joint DHS/USDA National Strategy for Foreign Animal Disease

At the request of the Congressional Appropriations Committees for both DHS and the Department of Agriculture (USDA), the two departments have coordinated a report on a national strategy for foreign animal disease. Participants in the joint study included DHS

(S&T), USDA (the Agricultural Research Service and the Agriculture and Plant Health Inspection Service), and stakeholder groups. The joint study has prompted an end-to-end review of the national response strategy following the identification of a case of foot-and-mouth disease, including the R&D requirements and gaps for assays, diagnostics, vaccines, and antivirals. Comprehensive roadmaps have been developed for these research areas, in one-, three-, and five-year timeframes. These roadmaps are important elements of program planning for S&T.

Workshops on Comparative Analysis

S&T's Office of Comparative Studies has sponsored two workshops on identifying analysis techniques and information sources crucial for analyzing the interaction of the terrorist threat with S&T activities. These workshops brought together participants from two DHS directorates, other government entities, academia and private industry and have helped to improve communication between these groups. Important analytical techniques and sources of information were identified and have been utilized. The workshops were also used to establish a set of topics which the office could profitably study. A proposal is being prepared which will solicit work on several of these topics.

Homeland Security Institute, and Homeland Security Science and Technology Advisory Committee

Homeland Security Institute

A formal solicitation was issued in December for the Homeland Security Institute (HSI), and proposals were received in January 2004. Those proposals currently are being evaluated with an expected five-year award by early May 2004. However, current legislation states that the Institute's operation will terminate in November 2005; this issue is of concern to the bidders.

The HSI was mandated by the Homeland Security Act to assist the Secretary and the Department in addressing important homeland security issues that require scientific, technical, and analytical expertise. The Institute will provide a dedicated, high-quality technical and analytical support capability for informing homeland security decision making at all levels. This capability will consist of an extensive program of operational assessments, systems evaluations, technical assessments, and resource analyses comparable to the capability developed and used for decades by the Defense establishment. The Institute will also provide analytical and technical evaluations that support DHS implementation of the SAFETY Act. Finally, the Institute will create and maintain a field operations program that will help further introduce real-world needs and experiences into homeland security is a disciplined and rigorous way.

Homeland Security Science and Technology Advisory Committee

The Homeland Security Science and Technology Advisory Committee (HSSTAC) was formally established in December 2003 and holds its first meeting in February 2004.

The HSSTAC was mandated by the Homeland Security Act to be a source of independent, scientific and technical planning advice for the Under Secretary for Science and Technology. The committee will (1) advise the Undersecretary on the mission goals for the future; (2) provide advice on whether the policies, actions, management processes, and organization constructs of the Science and Technology Directorate are optimally focused on mission objectives; (3) provide advice on whether the research, development, test, evaluation, and systems engineering activities are properly resourced (capital, financial, and human) to accomplish the objectives; (4) identify outreach activities (particularly in accessing and developing, where necessary, the industrial base of the Nation); and (5) review the technical quality and relevance of the Directorate's programs.

Countermeasures to Man-Portable Air Defense Systems

The S&T Directorate has selected three firms to provide analyses of the economic, manufacturing and maintenance issues needed to support a system to address the potential threat of MAN-Portable Air Defense Systems (MANPADS) to commercial aircraft. The next phase of the program will include development of prototypes using existing technology which will be subjected to a rigorous test and evaluation process. This initiative is not intended to develop new technology, but rather to re-engineer existing technology from military to commercial aviation use.

University and Fellowship Programs

Fellowships and Scholarships

In September 2003, the S&T Directorate named 100 students to the inaugural class of the Department of Homeland Security's Scholars and Fellows Program. The program, which received more than 2,400 applications, supports United States students who choose to pursue scientific careers and perform research in fields that are essential to the homeland security mission. The first class consists of 50 undergraduate students and 50 graduate students who are attending universities across the country majoring in the physical, biological, and social and behavioral sciences including science policy, engineering, mathematics, or computer science. The Directorate has already issued a notice inviting applications from students for the 2004-2005 academic year. The website is http://www.orau.gov/dhsed/.

University Centers of Excellence

The Science and Technology division has created the Homeland Security Centers Program that supports university-based centers of excellence dedicated to fostering homeland security mission critical research and education. The program has established the first Center of Excellence focused on risk analysis and modeling related to the economic consequences of terrorism at the University of Southern California, partnering with the University of Wisconsin at Madison, New York University and the University of California at Berkeley. A request for proposals has been issued for the second and third Centers of Excellence, which will focus on animal-related and post-harvest food agro-terrorism.

Homeland Security Advanced Research Projects Agency

Near-Term Technologies

In May 2003, the Science and Technology Directorate's Homeland Security Advanced Research Projects Agency (HSARPA) released a Broad Agency Announcement through the Technical Support Working Group for near-term technologies that can be rapidly prototyped and deployed to the field. A total of 3,344 responses as received in the following broad categories: chemical, biological, radiation and nuclear countermeasures; personnel protection; explosives detection; infrastructure protection; physical security; improvised device defeat; and investigative support and forensics. The first contract award went to North Carolina State University for the development of the next-generation of structural fire fighting personal protective equipment.

Detection Systems

The S&T Directorate reviewed and selected proposals for funding in response to its Research Announcement for Detection Systems for Biological and Chemical Countermeasures, which was published through the Technical Support Working Group. In September 2003, the Homeland Security Advanced Research Projects Agency (HSARPA) held its first Bidders Conference in Washington, DC. Approximately 420 private sector and university representatives attended the event and over 500 white papers were submitted. Finalists have been selected for negotiation, and work has already begun in a number of the more important areas.

Virtual Cyber Security Center

On December 13, 2003, a Request for Proposals and Statement of Work for technical and administrative support for the virtual Cyber R&D Center was published to seven capable performers listed on the GSA schedule. The deadline for response was December 15, 2003, and two responsive proposals were received. A three million dollar technical, management, and administrative contract was awarded to SRI International on February 2, 2004, to support the functions of the HSARPA Cyber R&D Center. The Cyber R&D

Center will be the primary S&T interface with the academic and industrial cyber security research communities.

Small Business Innovation Research (SBIR) Program Solicitation

On November 13, 2003, the Homeland Security Advanced Research Projects Agency (HSARPA) issued a Small Business Innovation Research (SBIR) Program Solicitation. The purpose of this solicitation was to invite small businesses to submit innovative research proposals that address eight high-priority DHS requirements:

- New system/ technologies to detect low vapor pressure chemicals (e.g., Toxic Industrial Chemicals)
- Chemical and biological sensors employing novel receptor scaffolds
- Advanced low cost aerosol collectors for surveillance sensors and personnel monitoring
- Computer modeling tool for vulnerability assessment of U.S. infrastructure
- Ship compartment inspection device
- Marine Asset Tag Tracking System
- Automatic Identification System tracking and collision avoidance equipment for small boats
- Advanced Secure Supervisory Control and Data Acquisition (SCADA) and related distributed control systems.

By the December 15, 2003, deadline 374 proposals had been received. The evaluation is complete and 66 proposers entered negotiation for Phase I contracts beginning February 11, 2004.

International Programs

Agreement with Canada on Border and Infrastructure Security

On October 3, 2002, Secretary Tom Ridge and Canadian Deputy Prime Minister John Manley initialed an agreement on Science and Technology Cooperation for protecting shared critical infrastructure and enhancing border security. The S&T Directorate is participating in a Working Group to develop near-term deliverables and projects to protect shared critical infrastructure such as bridges, dams, pipelines, communications and power grids; to develop surveillance and monitoring technologies to enhance the ability to disrupt and interdict terrorists; and to develop technologies for detecting the illicit transportation of chemical, biological, radiological, and nuclear weapons.

Weapons of Mass Destruction and Incident Management

Between March and December of 2003, the Office of Weapons of Mass Destruction Operations and Incident Management (WMDO-IM) provided surveillance and operational incident response to the Homeland Security Operations Center and law enforcement officials on 24 separate occasions. In addition, the WMDO-IM provided operational support to the Homeland Security Operations Center during Hurricane Isabel and the Northeast blackout.

The WMDO-IM established a scientific reach-back and rapid decision support capability through the Scientific and Technical Analysis and Response Teams (START). In addition to activating the START teams during the Code Orange time period in December 2003, WMDO-IM provided technical expert consultations on threats to the nation's water resources and responded to concerns about impacts of solar flares

WMDO-IM helped develop the Initial National Response Plan (INRP) and its National Incident Management System; the INRP represents a significant first step towards an overall goal of integrating the current family of Federal domestic prevention, preparedness, response, and recovery plans into a single all-discipline, all-hazards plan.

WMDO-IM provided technical support to the Homeland Security Operations Center (HSOC), assessing vulnerabilities and actions the HSOC can take to improve the ability to resist a chemical or biological terrorist attack

WMDO-IM, with the Defense Threat Reduction Agency and Nuclear Regulatory Commission, developed curriculum for a week-long training workshop on weapons of mass destruction for the Central Intelligence Agency University. Also in the area of education and training, WMDO-IM established a homeland security medical executive training course.