

**DEPARTMENT OF HOMELAND SECURITY
APPROPRIATIONS FOR FISCAL YEAR 2005**

TUESDAY, MARCH 2, 2004

U.S. SENATE,
SUBCOMMITTEE OF THE COMMITTEE ON APPROPRIATIONS,
Washington, DC.

The subcommittee met at 10 a.m., in room SD-124, Dirksen Senate Office Building, Hon. Thad Cochran (chairman) presiding.
Present: Senators Cochran, Stevens, and Byrd.

DEPARTMENT OF HOMELAND SECURITY

STATEMENTS OF:

**DR. CHARLES E. McQUEARY, UNDER SECRETARY, SCIENCE AND
TECHNOLOGY DIRECTORATE
LIEUTENANT GENERAL FRANK LIBUTTI, UNDER SECRETARY, IN-
FORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION**

OPENING STATEMENT OF SENATOR THAD COCHRAN

Senator COCHRAN. The meeting will please come to order.

We appreciate very much the attendance of our witnesses at today's hearing. We continue our review, today, of the fiscal year 2005 budget request for the Department of Homeland Security, with specific consideration being given to the programs and activities of the Science and Technology Directorate, and the Information Analysis and Infrastructure Protection Directorate.

I am pleased to welcome the Under Secretary for Science and Technology, Dr. Charles E. McQueary, and the Under Secretary for Information Analysis and Infrastructure Protection, Lieutenant General Frank Libutti.

The President is requesting \$1.04 billion for Science and Technology, and \$865 million for Information Analysis and Infrastructure Protection.

We appreciate the witnesses submitting their statements in advance. They will be printed in the hearing record and we invite you to make any remarks that you think would be helpful to the Committee's understanding of the budget request. But before proceeding, I want to yield to my distinguished friend and colleague, Senator Robert C. Byrd, for any opening statement that he may wish to make.

Senator BYRD. Thank you, Mr. Chairman.

Welcome, Mr. Under Secretary McQueary and Mr. Under Secretary Libutti.

Oh, by the way, Happy Birthday. Happy Birthday.

Dr. McQUEARY. Thank you.

HOW IAIP FUNDS ARE BEING SPENT

Senator BYRD. Over 1 year ago, the Information Analysis and Infrastructure Protection Directorate was established to enhance the sharing of threat information amongst all levels of Government and the private sector, to assess vulnerabilities of our critical infrastructure sectors, and to provide resources to protect them. However, it has been quite difficult for this subcommittee to receive information on what your budget is being spent on, or how the funding is being awarded.

I understand that our staffs had a constructive meeting yesterday, and I hope that this cooperation will continue. Not only do we hope it, but we expect it to continue.

CRITICAL INFRASTRUCTURE PROTECTION

When it comes to protecting this Nation's critical infrastructure, the Administration tells us that the private sector is taking care of it. Yet, there is no mandate on the private sector to make investments in security. Their involvement is voluntary. There are no benchmarks for Congress to use in assessing the private sector's role in critical infrastructure protection.

And so that is why, today, I am sending a letter asking the General Accounting Office, which is an arm of the Congress, to provide this subcommittee with an assessment of private sector investments to improve the security of our critical infrastructure such as chemical plants and ports since September 11, 2001.

INFORMATION ANALYSIS

Regarding information analysis, it is a mystery to me why this Administration, which celebrated the creation of this new department as a great success, has gone to great lengths to splinter its functions in the area of intelligence.

The President created the Terrorist Threat Integration Center, but gave primary responsibility to the CIA. He followed up this decision by establishing the Terrorist Screening Center within the FBI, creating further confusion about this Department's role in intelligence sharing.

Experts who follow this situation are concerned. The Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, better known as the Gilmore Commission, concluded in December that the IAIP directorate "does not have significant analytical power" to do what it takes, to analyze and disseminate intelligence information.

IAIP STAFFING

In the area of staffing, the IAIP directorate is barely keeping its head above water. After a year in existence, IAIP is struggling to meet its staffing goals. My understanding is that very few of the authorized intelligence analysts are on board.

SCIENCE AND TECHNOLOGY BUDGET

Let me turn now to Science and Technology. The Science and Technology Directorate's budget is the eighth largest R&D budget in the Federal Government. The budget request for fiscal year 2005

is just over \$1 billion. There is concern whether this budget is sufficient to address the various threats that we face, such as a biological, chemical or radiological attack.

Last year this subcommittee received hundreds of requests from members for research and technology projects at major universities. Rather than earmark projects, the subcommittee significantly increased the university account and allowed the department to select projects through a competitive process. Unfortunately, the President responded to this approach by proposing to substantially reducing funding for this purpose next year.

I look forward to hearing from our witnesses on why this cut is appropriate.

Mr. Chairman, I beg you to pardon my tardiness and I thank you for allowing me to proceed with my opening statement.

Senator COCHRAN. Dr. McQueary, we have a copy of your statement and we invite you to make any comments and remarks about the budget request which you think would be helpful to our understanding of the request that you're making.

You may proceed.

STATEMENT OF DR. CHARLES E. MCQUEARY

Dr. MCQUEARY. Thank you, Chairman Cochran. And Senator Byrd.

It's been several months since I have appeared before you and I welcome the opportunity to do so again.

It is a pleasure to be here today and have a chance to talk about 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 support the efforts of the dedicated men and women who protect and secure our homeland.

HIGHLIGHTS OF ACCOMPLISHMENTS

When I first reported to you about activities last year, we had just begun our work. The Directorate has accomplished much since its inception last March. And I would like to give you a few brief highlights, and several others are included in the written testimony that I have submitted.

First, we have deployed monitoring systems that operate continuously to detect biological pathogens in approximately 30 cities in the United States. We have also set up test beds to provide accurate radiation and nuclear warnings at air and marine cargo points, ports in cooperation with the Port Authority of New York and New Jersey. We have established the first series of interoperability guidelines for the Nation's wireless emergency communications network.

In another effort, we have greatly reduced the time it takes to develop national standards for technologies to protect the homeland.

Our new standards for radiation detection equipment will help put needed technologies into the hands of first responders quickly. And, our Homeland Security Advance Research Project Agency, or

HSARPA, has started extensive research for next generation biological and chemical, as well as radiological and nuclear detectors.

We have awarded the first round of 100 Homeland Security fellowships and scholarships to build U.S. leadership in science and technology. And we have also established the first university-based Homeland Security Center of Excellence to address both the targets and means of terrorism. And, we have become active contributors in numerous inter-agency working groups throughout the Federal Government.

In accomplishing this, we have doubled the staff of this directorate with some of the country's brightest and most dedicated people. We started the Directorate on March 1, last year, with 87 people and 53 of those were transferred in bulk from the Environmental Measurements Laboratory in Manhattan, New York. So the basic staff was quite small for carrying the program that we had responsibility for forward. Today, we are at about 210 people, which is exactly where we had hoped to be on our plan of adding staff to the organization.

However, as we all know, the threats to our homeland remain diverse and daunting. We must constantly monitor current and emerging threats, and assess our vulnerabilities to them. And we must develop new and improved capabilities to counter them, and be prepared to respond to and recover from a potential attack.

PRIORITIZATION OF RESEARCH AND DEVELOPMENT EFFORTS

The Science and Technology Directorate has prioritized its research and development efforts based on the directives and recommendations of many sources, including the Homeland Security Act of 2002, President Bush's National Strategy and nine Homeland Security Presidential Directives as well as the report of the National Academies of Science on making the Nation safer, and reports from the Gilmore, Bremer, and Hart-Rudman Committees.

We have identified and integrated the information in these sources for review and evaluation by our scientific staff, and it provides the basis for determining the Research and Development needed to meet our mission.

We recognize that many organizations are contributing to the Homeland Security's Science and Technology base. Congress recognized this as well and 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 began this coordination process by evaluating and producing a report on the Department of Homeland Security research and development activities underway that were not under the direct cognizance of the Under Secretary for Science and Technology. Where appropriate, Science and Technology will absorb these research and development functions in this fiscal year.

We are now initiating the effort needed to coordinate Homeland Security research and development across the entire United States Government. Discussions are ongoing with the Federal departments and agencies, as well as the Office of Management and

Budget, the Office of Science and Technology Policy, and the Homeland Security Council to ensure the best possible coordination.

FISCAL YEAR 2005 PLANS

At this time, I would like to briefly describe our fiscal year 2005 plans. We have an overall budget request of \$1.04 billion, which you identified, which is an increase of \$126.5 million or about 14 percent over fiscal year 2004. With these funds Science and Technology will continue to make progress in securing the homeland.

For example, under President Bush's new biological-surveillance initiative, which accounts for most of the increase in funding, additional capability will be implemented quickly in the top-threat urban areas to provide more than twice the current capability.

We will continue to provide the science and technology capabilities and enduring partnerships needed to develop methods and tools to test and assess threats and vulnerabilities to protect our critical infrastructure and enhance information exchange.

We will continue to work in cyber security both through partnerships and by creating low-cost and high impact solutions to identified cyber security challenges. And of course, this is done in concert with my good friend, General Libutti.

We will wrap-up our work in counter-MANPADS to improve technology to protect commercial aircraft from the man-portable air defense systems or the shoulder-fired missiles, which present a vulnerability to our commercial aircraft industry.

We will award contracts in fiscal year 2005 for integrating commercial prototype equipment on selected commercial aircraft and conduct test evaluation including a live-fire range test.

In conclusion, this year the scientists and engineers in the Science and Technology Directorate have accomplished more than I could have expected. I am proud to have shared some of these success stories with you today. We have appended a more comprehensive summary of the accomplishments to date for the record.

PREPARED STATEMENT

Yet, we also recognize that there is much more to do and we will be working just as hard in fiscal year 2005. I look forward to working with you, with my colleagues in other Federal agencies, and with private industry and academia to continue this work and improve our ability to protect our homeland and our way of life.

This concludes my prepared statement, and I will be prepared to answer questions at the appropriate time.

[The statement follows:]

PREPARED STATEMENT OF DR. CHARLES E. MCQUEARY

INTRODUCTION

Good morning. Chairman Cochran, Senator Byrd, 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:

- deployed continuously operating biological pathogen detection systems to approximately 30 United States cities;
- 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;
- established the first series of interoperability guidelines for the Nation's wireless emergency communications network;
- established the first national standards guidelines for radiation detection equipment;
- awarded the first Homeland Security Fellowships and Scholarships;
- established the first Homeland Security University Center of Excellence;
- transferred the Plum Island Animal Disease Center from the Department of Agriculture to the Science and Technology Directorate;
- 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;
- 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;
- 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 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 fiscal year 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 lit-

tle 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 FISCAL YEAR 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 United States government's E-Gov Initiatives, the SAFECOM Program. There are tens of thousands of State and local public safety agencies, and 100 Federal law enforcement agencies that depend on interoperable wireless communications. The SAFECOM (Wireless Public SAFETy Interoperable COMMunications) program is the umbrella initiative to coordinate all Federal, State, local, and Tribal users to achieve national wireless communications interoperability. 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 fiscal year 2005 plans. As can be seen in the following chart, we have an overall fiscal year 2005 budget request of \$1.039 billion, which is an increase of \$126.5 million (13.9 percent) over the fiscal year 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 to enhance and expand the BioWatch Program.

[Dollars in millions]

Budget activity	Fiscal year 2003 Amount	Fiscal year 2004 less rescission Amount	Proposed fiscal year 2005 Amount	Increases/Decreases from fiscal year 2004 to 2005	
				Amount	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

[Dollars in millions]

Budget activity	Fiscal year 2003 Amount	Fiscal year 2004 less rescission Amount	Proposed fiscal year 2005 Amount	Increases/Decreases from fiscal year 2004 to 2005	
				Amount	Percent increase
Bio Countermeasures (incl. NBACC)	362.6	285.0	407.0	122.0	42.8
High-Explosives Counter- measures	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 Pro- grams	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 appropria- tions and budget esti- mates	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 fiscal year 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 fiscal year 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 significant deterrent role, since terrorists are less likely to attack when they know that defensive systems prevent them from attaining their goals.

Established the National Biodefense Analysis and Countermeasures Center, which provides scientific support for intelligence activities, prioritizes biothreats, and conducts bioforensic analyses for attribution and hence deterrence.

In fiscal year 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 fiscal year 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 fiscal year 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 fiscal year 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 fiscal year 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 (3-year), and long-term (5-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 fiscal year 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 fiscal year 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 fiscal year 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 fiscal year 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, 3-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 fiscal year 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 fiscal year 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.
- 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 fiscal year 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 Depart-

ments of Energy, Defense, Justice, and Agriculture, the intelligence community, and the National Institutes of Health.

In fiscal year 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 fiscal year 2005, we will leverage the activities started during fiscal year 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 fiscal year 2003 and fiscal year 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 fiscal year 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 fiscal year 2003 and fiscal year 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 solu-

tions 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 fiscal year 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 fiscal year 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 fiscal year 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 fiscal year 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 HAWK-EYE 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 fiscal year 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 fiscal year 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 just under 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 fiscal year 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 fiscal year 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 3-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 all Federal, State, local, and Tribal users to achieve national wireless communications interoperability. 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.

Since the Science and Technology Directorate formally assumed responsibility for the management of the SAFECOM program barely 7 months ago:

- SAFECOM has been established as the one umbrella group in the Federal Government for the management of public safety wireless interoperability programs;
- 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;
- A Federal coordinating structure has, for the first time, been created to coordinate all Federal public safety wireless interoperability programs;

- The first catalog of national programs touching on public safety wireless interoperability has been developed and published; and
- 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 fiscal year 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. 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.

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. 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	Fiscal year 2005 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=10E-4, Multiplex 10 assays
Fiscal year 2005 milestones: Decontamination technologies and standards for facilities and outdoor areas. National Academy of Science study characterizes contamination risks.	Milestones will be achieved
Fiscal year 2005 milestones: Establishment of a national capability in bio-defense 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. Fiscal year 2005 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	Fiscal year 2005 target
Fiscal year 2005 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	Fiscal year 2005 target
Fiscal year 2005 milestone: Pilot tests of standoff detection technologies	Milestone will be achieved

ST0004 Radiological & Nuclear Countermeasures

Long term performance goal.—By fiscal year 2009, an effective suite of countermeasures against radiological and nuclear threats will be developed with capabilities in detection, intelligence analysis, response, and preparedness.

Performance measures	Fiscal year 2005 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 fiscal year 2004.	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	Fiscal year 2005 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	Fiscal year 2005 target
Long-term implementation of SAFETY Act Fiscal year 2005 milestones: Technical standards and test/evaluation protocols will be established for WMD decontamination technologies and analysis tools. “Consumer’s report” on radiation and bioagent detection devices for Federal, State, and local users will be published.	Certifications Milestones will be achieved

ST0008 Homeland Security Fellowship Programs/University Programs

Long term performance goal.—Significantly increase the number of U.S. students in fields relevant to homeland security including the physical life and social sciences; and engineering.

Performance measures	Fiscal year 2005 target
To increase the nation’s science and technology workforce and research capability on issues related to homeland security. Fiscal year 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	Fiscal year 2005 target
Improved capability to prevent terrorist attacks through annual emerging threat assessment report (percent 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	Fiscal year 2005 target
Technologies prototyped or commercialized	3

ST0011 SAFECOM

Long term performance goal.—Provide public safety agencies with central coordination, leadership and guidance to help them achieve short-term interoperability and long-term compatibility of their radio networks across jurisdictions and disciplines.

Performance measures	Fiscal year 2005 target
Increased interoperability across local, tribal, State, and Federal public safety jurisdictions and disciplines. Fiscal year 2005: Based on fiscal year 2004 baseline, improvements in 3 categories	3

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	Fiscal year 2005 target
Effective technology/technologies for commercial aircraft to defeat man-portable anti-aircraft missiles identified. Fiscal year 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	Fiscal year 2005 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 11 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 dollars]

Fiscal year	Fiscal year (actual)	Fiscal year 2004 (estimated)	Fiscal year 2005 (proposed)
Basic	47	117	80
Applied	59	56	229
Developmental	398	608	643
Total	504	781	952
Percent 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: BIEWATCH 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 2 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 fiscal year 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 fiscal year 2004 R&D activities.

The fiscal year 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 (\$13.5 million); Emergency Preparedness and Response RDT&E activities supporting the U.S. Fire Administration (\$0.65 million); and ICE-Federal Air Marshall's RDT&E activities supporting the development of their Air-to-Ground Communication System (\$10 million).

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 fiscal year 2005 is \$18 million.

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 staff 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 Science and Technology Directorate has identified separate mechanisms to access the capability base at the DOE national laboratories and sites to guard against organizational conflicts of interest and inappropriate use of inside information in responding to competitive private sector solicitations. Five national laboratories (Livermore, Los Alamos, Oak Ridge, Pacific Northwest, and Sandia) have been identified as Intramural Laboratories. These labs will help S&T set research goals and

requirements and formulate R&D road maps. This level of engagement would give the intramural labs unfair advantage if they were permitted to compete for funding awarded through open solicitations.

All other DOE laboratories and sites have been identified as Extramural Laboratories. Because the Extramural Laboratories will not be involved in internal DHS research planning, they are eligible to compete in Homeland Security Advanced Research Projects Agency (HSARPA) and Systems Engineering and Development (SED) funding, such as the Broad Agency Announcement (BAA) valued at \$50 million for radiological/nuclear technologies that was recently issued. The majority of the Science and Technology Directorate's funding will be executed through HSARPA and SED. These labs may also freely team with industrial partners to seamlessly commercialize technologies they have developed.

BUDGET FOR UNIVERSITY CENTERS OF EXCELLENCE AND FELLOWS PROGRAMS

The President's fiscal year 2005 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. If more than a total of three Centers of Excellence are desired without increasing the President's fiscal year 2005 budget request, a reduction in the scholars and fellows program would be required.

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 less than 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 fiscal year 2005.

I look forward to continuing to work with you on the Cybersecurity, Science, and Research & Development Subcommittee; 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, Senator Byrd, 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

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 re-

sponse 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.

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 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 is providing seed money for the Department of Justice's 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 Federal resource needs, 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 ensure that every vendor has a fair opportunity to participate.

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 \$5.45 million, 3-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, Berkeley.

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 3-year, \$5.6 million, 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 U.S. 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 \$2.4 million for fiscal year 2003 and \$5 million for fiscal year 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 1-, 3-, and 5-year timeframes. These roadmaps are important elements of program planning for S&T.

National Security Council Attribution Working Group

The S&T Directorate initiated and leads the National Security Council Attribution Working Group, which is revisiting national capabilities to rapidly perform forensic analysis in cases of nuclear and radiological events of any size. This effort is expected to lead to a robust and completely coordinated forensic capability for attribution.

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 5-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 in 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.

SAFECOM Vendor Demonstration Day

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.

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.

Senator COCHRAN. Thanks, Dr. McQueary.
General Libutti, you may proceed.

STATEMENT OF LIEUTENANT GENERAL FRANK LIBUTTI

General LIBUTTI. Good morning, Chairman Cochran, and Senator Byrd.

I am delighted to appear before you today to discuss the President's fiscal year 2005 budget request for the Department of Home-

land Security's Information Analysis and Infrastructure Protection Directorate. And I look forward to a meeting with you soon to discuss the classified portion of the Information Analysis and Infrastructure Protection budget, specifically, the intelligence side of business.

Information Analysis and Infrastructure Protection is the focal point for intelligence, analysis, and infrastructure protection operations and information sharing within the Department of Homeland Security. Within a single Directorate, IAIP merges capability to identify and assess a broad range of intelligence and information concerning threats to the homeland, maps the information against the Nation's vulnerabilities, issues timely and actionable warnings, and takes appropriate preventive and protective action to protect our infrastructure and key assets.

ACCOMPLISHMENTS OF THE IAIP DIRECTORATE

As we mark the first anniversary of the Department, I would like to highlight for you some of the many accomplishments of our IAIP Directorate.

Since March 2003, IAIP has launched the Homeland Security Information Network, a comprehensive interactive information sharing program that expands access to and use of a joint regional information exchange system. The roll out includes all of our partners at the State and local levels, as well as private sector partners.

Next, we have implemented the Homeland Security Presidential Directive HSPD-7 which addresses critical infrastructure identification, prioritization and protection. And as you know this was signed by President Bush in December of 2003.

To the National Cyber Security Division, the NCSD, we have established the U.S. Computer Emergency Readiness Team, or USCERT, and launched the National Cyber Alert System, America's first coordinated cyber security system for identifying, analyzing and prioritizing emerging vulnerabilities and threats. This system provides the first nation-wide infrastructure for relaying actionable computer security updates and warning information to computer users in the Government, the private sector, business, and home users as well.

We've assumed the responsibility for the Homeland Security Operation Center, which maintains and shares real-time domestic situation awareness, coordinates security operations, detects, prevents and deters incidents, and facilitates response and recovery for all critical incidents and threats.

In addition, we have conducted detailed vulnerability studies of the banking and telecommunication industries to better understand the inter-dependencies therein, and prioritization regarding vulnerability reduction.

We formally executed the Protected Critical Information Infrastructure Protection Program. This is pursuant to the provisions of the Critical Information Infrastructure Information Act of 2002.

Even with these accomplishments there is much more work to be done. IAIP's budget relies on the expectation of two emerging trends. First, the nature and complexity of the threats which will increase. And second, our national infrastructure components

which will become more complex and more interdependent. These trends will result in more demands on the department and IAIP to anticipate terrorist intentions, tactics and capabilities, and to mitigate risks and vulnerabilities for the protection of the United States of America and its citizens.

FISCAL YEAR 2005 BUDGET REQUEST FOR IAIP

For these reasons, the President's fiscal year 2005 budget request for IAIP is structured around the following major programs: Threat determination and assessments; Infrastructure vulnerabilities and risk assessments; Information warnings and advisories; Remediation and protective actions; Outreach and partnerships; National Communication System; Competitive analysis and evaluation; National plans and strategies; and the Homeland Security Operation Center.

Let me discuss several of the initiatives associated with each of the mission areas of the fiscal year 2005 request for \$864 million.

THREAT DETERMINATION AND ASSESSMENT

First, threat determination and assessment. Funding in this area is targeted to increase the IAIP directorate's technology competencies by training analysts and equipping IAIP with the most advanced technologies and tools.

The training tools and technology will be utilized to develop a detailed understanding of terrorists' organizational capabilities with supporting materials and conductivity to interpret and predict threats.

Next, is to expand cooperation and fusion efforts from Homeland Security to our internal components and out to external customers, and increase cooperation efforts among the intelligence community.

INFRASTRUCTURE VULNERABILITY AND RISK ASSESSMENT

Next, the infrastructure vulnerability and risk assessment piece. This funds the development of comprehensive national infrastructure risk analysis and profile. There we are talking about high-value target sets, the development of analytic tools to evaluate critical infrastructure and key assets, and the coordination of a national threat vulnerability and asset database to assess, integrate, collaborate and store threat vulnerability information.

Next, information and warning advisories. In addition to continuously operating a 24/7 Capable Operations Center, the information and warning program will provide search capability for our HSOC, our operation center, and for other directorates during heightened states of alert or in response to specific incidents.

Funding in this area supports submission of collection requests for threat information of the intelligence community, the law enforcement, and dissemination guidance to Homeland Security components, developing analysis on the nature and scope of the threat, and identifying potential terrorists' targets within the United States.

Another priority is the need to establish threat advisories, bulletins and warnings at different levels of classification to relevant stakeholders. The threat publications are detailed and dissemi-

nated in a timely fashion portraying the nature, scope and target of the threat.

REMEDICATION AND PROTECTIVE ACTIONS

Next, remediation and protective actions. Through this program the IAIP directorate provides a broad range of services including on-site planning advice, technical and operational training programs, assistance in identifying vulnerabilities and development of sharing and best-practices. Activities in this area also include security efforts to protect infrastructure and key assets from cyber attacks.

Specifically, the \$345.783 million for remediation and protective actions is divided into the following five categories: Critical infrastructure and key asset identification; Critical infrastructure of vulnerability field assessments; Infrastructure and key asset protection; Cyber security; and last, protection standards and performance matrixes.

OUTREACH AND PARTNERSHIP

The next broad category is outreach and partnership. The fiscal year 2005 President's budget requests \$40.829 million to build and maintain a sound partnership foundation. To be successful in information sharing, strong relationships must be maintained with State and local governments, private sector, academia, advisory bodies and the international community.

NATIONAL COMMUNICATION SYSTEM

Next, the national communication system. This allows NCS to ensure priority use of telecommunication services during times of national crisis, including the government emergency telecommunication service, GETS. The funding enhances these programs and supports the development of wireless priority services, which provide a nationwide priority cellular service to key national security and emergency preparedness users.

COMPETITIVE ANALYSIS AND EVALUATION

Next, competitive analysis and evaluation. The competitive analysis and evaluation program ensures that IAIP products and services are tested and accurate based on sound assumptions and data, and ultimately offers the highest quality, depth and value to the IAIP customers.

NATIONAL PLANS AND STRATEGIES

Next is our national plans and strategies. Critical to ongoing national efforts to protect and ensure the homeland, our actions support updating, coordinating and monitoring the implementation of national plans and strategies.

HOMELAND SECURITY OPERATION CENTER

Homeland Security Operation Center, \$35 million. The HSOC or Homeland Security Operation Center maintains and shares domestic situational awareness, coordinates security operations, protects,

prevents and deters incidents, and facilitates the response and recovery of all critical incidents.

The HSOC is the focal point for sharing information across all levels of government, the private sector and our friends at the State and local levels as well.

PREPARED STATEMENT

In summary, the fiscal year 2005 budget request provides the resources to enable IAIP to manage and grow in its mission of securing the homeland. I look forward to working with you to accomplish the goals of this department and the goals of IAIP.

Mr. Chairman, Senator Byrd, this concludes my prepared statement and I would be happy to answer any questions you may have at this time. Thank you.

[The statement follows:]

PREPARED STATEMENT OF FRANK LIBUTTI

Introduction

Good morning Chairman Cochran, Senator Byrd and distinguished members of the Subcommittee. I am delighted to appear before you today to discuss the President's fiscal year 2005 budget request for the Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) Directorate.

IAIP is the focal point for intelligence analysis, infrastructure protection operations, and information sharing within the Department of Homeland Security (DHS). Within a single directorate, IAIP merges the capability to identify and assess a broad range of intelligence and information concerning threats to the homeland, map that information against the nation's vulnerabilities, issue timely and actionable warnings, and take appropriate preventive and protective action to protect our infrastructures and key assets. IAIP is currently comprised of three primary components: the Office of Information Analysis (IA), the Office of Infrastructure Protection (IP), and the Homeland Security Operations Center (HSOC).

Fiscal Year 2004 Accomplishments

As we mark the first anniversary of the Department, I would like to highlight for you some of the many accomplishments of the IAIP Directorate, one of the newest parts of the Federal Government. The formation of IAIP has created for the first time a unique, integrated capability to not only map the current threat picture against the nation's vulnerabilities, but to also assess the risk of a terrorist attack based upon preventive and protective measures in place. That is, IAIP is enabling us to move from a reactive posture in the homeland to a risk management and mitigation posture. Let me give you some examples.

Since March, 2003, IA has:

- Launched the Homeland Security Information Network (HSIN), a comprehensive information sharing program that expands access to and use of the Joint Regional Information Exchange System (JRIES). The HSIN will provide secure real-time connectivity in a collaborative environment with States, urban areas, counties, tribal areas, and territories to collect and disseminate information between Federal, State, local, and tribal agencies involved in combating terrorism.
- Coordinated Operation Liberty Shield and the rapid enhancement of security at more than 145 national asset sites at the outset of the war in Iraq. Following that, IAIP transitioned the protection of the sites from National Guard and law enforcement to a more cost effective and permanent set of physical protective measures.
- Enhanced protection, by assisting local communities with conducting vulnerability assessments and implementing protective measures, of the nation's highest risk chemical sites, thereby improving the safety of over 13 million Americans.
- Implemented Homeland Security Presidential Directive (HSPD) 7, "Critical Infrastructure Identification, Prioritization and Protection," which was signed by President Bush in December 2003. The HSPD assigned the Department of Homeland Security responsibility for coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the

- United States and the development of an integrated cyber and physical protection plan.
- Implemented Wireless Priority Service, to ensure the continuity of cellular networks nationwide, registering over 3,000 Federal, State, local and private users.
 - Established the National Cyber Security Division (NCSA) to coordinate the implementation of the National Strategy to Secure Cyberspace and serve as the national focal point for the public and private sectors on cybersecurity issues, and developed a process for handling cyber incidents, successfully managing a number of major cyber events.
 - Through the NCSA, established the U.S. Computer Emergency Readiness Team (US-CERT) through an initial partnership with the Computer Emergency Response Team Coordination Center at Carnegie Mellon University. US-CERT is building a cyber watch operation, launching a partnership program to build situational awareness and cooperation, and coordinating with U.S. Government agencies to predict, prevent, and respond to cyber attacks.
 - Launched the National Cyber Alert System under the auspices of US-CERT, America's first coordinated cyber security system for identifying, analyzing, and prioritizing emerging vulnerabilities and threats. This system provides the first nationwide infrastructure for relaying actionable computer security update and warning information to computer users in the government, in private industry, and small business and home users.
 - Assumed responsibility for the Homeland Security Operations Center (HSOC), which maintains and shares real time domestic situational awareness; coordinates security operations; detects, prevents, and deters incidents; and facilitates response and recovery for all critical incidents and threats. As of February 2004, 26 Federal and local law enforcement agencies and Intelligence Community members are represented in the HSOC, providing reach back capability into their home organizations to continuously inform the current threat picture, and to provide key decision makers with real time information.
 - Conducted detailed vulnerability studies of the banking and telecommunications industry to better understand the interdependencies and prioritize vulnerability reduction.
 - Initiated an intra-Department and interagency review and analysis of information obtained in detainee briefings to assess specific terrorist capabilities, work that subsequently became the subject of several advisories disseminated to a variety of homeland security partners regarding terrorist planning, tactics and capabilities.
 - Co-chaired with the Border and Transportation Security Directorate (BTS) the DHS Intelligence Activities Joint Study charged with reviewing the mission, responsibilities and resources of DHS Intelligence component organizations. The study was chartered for the purpose of making recommendations to the Secretary as to the optimal utilization of the Department's analytical resources.
 - With the Homeland Security Council (HSC), initiated an ongoing interagency review of the Homeland Security Advisory System (HSAS), for the purpose of refining the system to make it more efficient and more beneficial for States and localities and the private sector.
 - Formally executed the Protected Critical Infrastructure Information (PCII) implementing regulation, pursuant to the provisions of the Critical Infrastructure Information ACT of 2002. The purpose of the PCII Program is to encourage private entities and others with knowledge about our critical infrastructure to voluntarily submit confidential, proprietary, and business sensitive critical infrastructure information to the Department through IAIP. Information submitted to IAIP that qualifies for protection under the provisions of the Act and the PCII implementing regulation will be exempted from public disclosure, providing a significant opportunity for private entities to assist in homeland security without exposing potentially sensitive and proprietary information to the public. The Department will use information that qualifies for protection primarily to assess our vulnerabilities, secure the nation's critical infrastructure and protected systems, issue warnings and advisories, and assist in recovery.

Fiscal Year 2005

Even with these accomplishments, there is much more work that must be done. The United States remains at risk, despite the continuing work to assess and mitigate vulnerabilities. Our interdependent critical infrastructures enable Americans to enjoy one of the highest standards of living in the world, provide the backbone for the production of goods and services for the world's largest economy, provide over 60 million jobs, and ensure the United States can protect its national security inter-

ests. Infrastructure will remain one of the top priority targets for terrorists desiring to damage the nation's economy and incite fear in the minds of the American people.

While the possibility of large-scale attacks similar to 9/11 remain significant, it is also possible likely that terrorists will employ smaller scale operations such as the suicide bombings prevalent in Israel. Terrorists understand that the cumulative effect of many small-scale operations—that are easier to plan and conduct—can be just as effective as large-scale attacks in their overall impact on Americans' sense of security in their own country and, especially, at United States facilities overseas.

IAIP's budget relies on the expectation of two emerging trends: First, the nature and complexity of threats will increase; and, second, our national infrastructure components will become more complex and interdependent. These trends will result in more demands on the Department and IAIP to anticipate terrorist intentions, tactics and capabilities, and to mitigate risks and vulnerabilities for the protection of the United States and its citizens.

For these reasons, the President's fiscal year 2005 budget request for IAIP is structured around the following major program areas: Threat Determination and Assessments, Infrastructure Vulnerabilities and Risk Assessments, Information Warnings and Advisories, Remediation and Protective Actions, Outreach and Partnerships, National Communications System, Competitive Analysis and Evaluations, National Plans and Strategies, and the Homeland Security Operations Center.

Threat Determination and Assessment (\$21.943 Million)

IAIP's Threat Determination and Assessment program is designed to detect and identify threats of terrorism against the United States homeland; assess the nature and scope of these terrorist threats; and understand terrorist threats in light of actual and potential vulnerabilities within critical infrastructures and/or key assets. Addressing these issues requires the IAIP Directorate to improve on its existing set of threat analysts and analytical tools by hiring and training additional highly skilled threat analysts; acquiring and fielding new analytical tools and technologies to assist in assessing and integrating information; and deploying secure communications channels that allow for the rapid exchange of information and dissemination of analytical results.

These improvements will be used for multiple purposes, including: (1) providing analysis and assessments of the current threat picture as it relates to critical infrastructure; (2) developing actionable intelligence for Federal, State, and local law enforcement; (3) issuing warnings at all levels from the Federal Government to the private sector; and (4) supporting efforts to identify and coordinate effective countermeasures.

The President's Budget requests \$21.943 million for continued support of on-going activities to continually form terrorist threat situational awareness, execute the functions outlined above, and focus on information sharing and coordination within DHS as well as in the Intelligence Community and other external stakeholder communities. These capabilities enhance the performance of two critical functions in protecting the homeland. First, it offers the United States Government the ability to integrate, synchronize, and correlate unique sources of information relating to homeland security, emanating from traditional and non-traditional (e.g., State and local governments, private industry) sources. Second, the IAIP Directorate is positioned to integrate knowledge of potential terrorist threats with an understanding of exploitable infrastructure vulnerabilities, resulting in a value-added profile of national risk that transcends traditional threat and vulnerability assessments.

Funding in this area is targeted to increase the IAIP Directorate's technical competencies by training analysts and equipping IAIP with the most advanced technologies and tools. The training, tools and technologies will be utilized in four primary areas:

- Model Terrorist Organization.*—Developing a detailed understanding of terrorist organization capability with supporting materials and connectivity to interpret and predict threats.
- Develop Terrorist Capabilities Baseline.*—Developing a detailed understanding of terrorist capabilities baseline with supporting materials and connectivity to interpret and predict threats.
- Collaboration and Fusion.*—Expanding collaboration and fusion efforts from DHS to internal components, and out to an extended customer base.
- Analysis Coordination.*—Spearheading the effort to build a collaborative and mutually supporting analysis coordination schematic for DHS, and ensure that it incorporates others (TTIC, TSC, and the Intelligence Community) into a "community of interest" approach for understanding domestic terrorist threats.

Infrastructure Vulnerability and Risk Assessment (\$71.080 million)

The Homeland Security Act directs the IAIP Directorate to carry out comprehensive assessments of the vulnerabilities of the critical infrastructure and key assets of the United States. As such, the IAIP Directorate serves as the focal point for coordination between the Federal Government, critical infrastructure owners and operators, and State and local governments for the sharing of information and the planning for response to crisis events affecting infrastructures.

The fiscal year 2005 President's Budget requests \$71.080 million to fund the development of a comprehensive National infrastructure risk analysis and profile (e.g., high value/high probability of success targets); development of analytic tools to evaluate critical infrastructure and key assets; and the coordination and development of a National threat vulnerability and asset database to access, integrate, correlate, and store threat and vulnerability information.

These mission areas will be enable IAIP to identify potential risks caused by infrastructure interdependencies, and determine the potential consequences of an infrastructure failure due to a terrorist attack. Ultimately, the intent of these efforts is to strengthen the capabilities of the IAIP Directorate and each critical infrastructure to provide near real-time notification of incidents; enhance the ability of the IAIP Directorate to assess the impact of incidents on critical infrastructure and key assets; to assess collateral damage to interdependent infrastructure; and create tools and processes to enhance infrastructure modeling and risk assessment capabilities.

The fiscal year 2005 budget request for infrastructure vulnerability and risk assessment is divided into three areas:

—*National Infrastructure Risk Analysis.*—Funding in this area supports the development of comprehensive risk and vulnerability analyses on a national scale. These analyses are cross-sector in nature, focusing on problems affecting multiple infrastructures, both physical and cyber-related. As assigned in the Homeland Security Act and HSPD-7, the IAIP Directorate will continue to leverage and develop new techniques to map data provided by threat analyses, provide consequence analysis, and create vulnerability assessment teams based on the nature of the indicators or incidents. The goal is to produce timely, actionable information that is more meaningful to industry. A portion of this funding also supports the direct involvement of critical infrastructure sector experts to supplement risk analysis efforts and to gain a better understanding of the sector's core business and operational processes. In addition, a portion of this funding is utilized for exploration and to pilot innovative methodologies to examine infrastructure vulnerabilities and interdependencies.

—*Analytic Tools Development and Acquisition.*—The IAIP Directorate will continue to collaborate with the Science and Technology (S&T) Directorate to acquire the most advanced tools and database designs available to better understand the complexities of interdependent systems and for translating vast amounts of diverse data into common and usable information for decision-makers, analysts, and infrastructure operators. Such capabilities include data-logging systems, modeling and simulation, data mining, and information correlation. Funding is targeted toward developing dynamic and multi-faceted tools designed to expand access to needed information.

—*National Threat/Vulnerability/Asset Databases.*—The funding level requested for this activity in the fiscal year 2005 budget is based on the recognition of the data intensive nature, scale and complexity of analyzing infrastructure vulnerability issues. The intent is to develop and maintain databases that allow the IAIP Directorate to provide its stakeholders with up-to-date information on threats and vulnerabilities. Specifically, the IAIP Directorate is continuing to coordinate and direct the development of the primary database of the Nation's critical infrastructures through a collaborative process involving all stakeholders; maintain data on the risks posed to specific facilities and assets (and the probability of attack and associated consequences for homeland, national, and economic security should an attack occur); and develop, operate, and manage integrated data warehouses—in full compliance with the Department's privacy policies—that contain comprehensive all-source threat, vulnerability, and asset data.

Information and Warning Advisories (\$59.807 Million)

One of the most visible aspects of the DHS mission lies in the management and administration of the Homeland Security Advisory System, the communications of threat condition status to the general public, and the continuous around-the-clock monitoring of potential terrorists threats. Specifically, there are three key information and warning activities that help support the Homeland Security Advisory System and other efforts to alert key Departmental leadership, national leaders and the

general public: (1) tactical indications and warning and the associated warning advisory preparation and issuance; (2) information requirements management; and (3) integrated physical and cyber infrastructure monitoring and coordination.

The fiscal year 2005 President's Budget requests \$59.807 million to maintain the information and warning program. In addition to continuously operating a 24x7 capability, the information and warning program area will provide surge capabilities for the HSOC and with other Directorates during heightened states of alert or in response to specific incidents. The relevant fiscal year 2005 budget request is divided into three primary areas:

—*Tactical Indications and Warning Analysis/Warning Advisory Preparation and Issuance.*—Funding in this area supports submission of collection requests for threat information to the Intelligence Community and law enforcement, disseminating guidance to DHS components, developing analyses on the nature and scope of the threats, and identifying potential terrorist targets within the United States. A program priority is the continued development of tools and technologies to assist our analysts to interpret, integrate, and catalogue indicators, warnings, and/or actual events and to provide Departmental and national leaders situational awareness. Another priority is the need to publish threat advisories, bulletins, and warnings at different levels of classification prior to distribution to the relevant stakeholders. Threat publications are detailed and disseminated in a timely fashion, portraying the nature, scope, and target of the threat. Ultimately, this information provides the basis for determinations to change the threat condition.

—*Information Requirements Management.*—Information related to threats and critical infrastructure vulnerabilities are collected, stored, and protected within a diverse set of locations and sources, spanning all levels of government (Federal, State, and local) and including intelligence, proprietary and public sources. Funding in this area supports the technologies necessary to search within those diverse databases to identify, distill, and/or acquire mission-critical information. Program funding supports efforts to coordinate information requests and tasks emanating from within other parts of IAIP, other DHS Directorates, the Intelligence Community, law enforcement, State and local governments, and the private sector. In addition, a portion of these funds is used to supplement the information technology structure to accomplish these tasks efficiently and effectively through the use of leading-edge capabilities. This effort ensures that all information users are able to access all available and relevant data.

—*Integrated Physical and Cyber Infrastructure Monitoring and Coordination.*—Intelligence and warning staff monitoring and coordination efforts ensure that threat and critical infrastructure issues are adequately addressed and represented. In addition, these efforts coordinate incident response, mitigation, restoration, and prioritization across critical sectors in conjunction with the other relevant DHS components (e.g., Emergency Preparedness and Response Directorate).

Remediation and Protective Actions (\$345.738 Million)

The IAIP Directorate has established a national Critical Infrastructure Protection program that leverages stakeholder input at the Federal, State, and local level and across the private sector to provide the best and most cost-effective protective strategies for “at risk” infrastructure and facilities. Through this program, the IAIP Directorate provides a broad range of services including on-site planning advice, technical and operational training programs, assistance in identifying vulnerabilities, and development and sharing of best practices. Activities in this area also include security efforts to protect infrastructure and assets from cyber attacks (e.g., malicious software, distributed denial-of-service attacks).

Specifically, the fiscal year 2005 President's Budget requests \$345.738 million, for remediation and protective actions divided into the following five areas:

—*Critical Infrastructure and Key Asset Identification.*—The Homeland Security Act directs the IAIP Directorate to recommend measures necessary to protect the critical infrastructure of the United States. One key step in this process is funding a national program focused on identifying critical infrastructure and assets and assessing potential risks of successful attacks to those assets. By understanding the full array of critical infrastructure facilities and assets, their interaction, and the interdependencies across infrastructure sectors, IAIP is able to forecast the national security, economic, and public safety implications of terrorist attacks and prioritize protection measures accordingly. Moreover, the process of identifying and prioritizing assets in this manner creates a common overarching set of metrics that consist of the individual attributes of specific infrastructure sectors.

- Critical Infrastructure Vulnerability Field Assessments.*—The Directorate coordinates with all relevant Federal, State and local efforts to identify system vulnerabilities and works closely with the private sector to ensure vulnerability field assessment methodologies are effective, easy to use, and consistently applied across sectors. Funding is targeted at the need to conduct and coordinate specialized vulnerability assessments by DHS teams, in conjunction with teams from other Federal or State agencies and private sector companies as appropriate, for the highest priority critical infrastructures and assets. The intent of these efforts is to catalogue specific vulnerabilities affecting the highest priority terrorist targets, thereby helping guide the development of protective measures to harden a specific facility or asset. A nationwide vulnerability field assessment program is currently underway leveraging the expertise of the IAIP Directorate, other agencies, and the private sector to ensure cross-sector vulnerabilities are identified and that sound, informed decisions will be reached regarding protective measures and strategies.
- Infrastructure and Key Asset Protection Implementation.*—Due to the vast geographic size of the United States and diverse operating environment for each infrastructure sector, protection strategies must start at the local level and then be applied nationally as needed. Priorities for protection strategies are based on regional, State, and local needs and on the need for cross-sector coordination and protective actions within those geographic boundaries. The budget request reflects the need for the IAIP Directorate to continue the development of a flexible set of programs to assist in the implementation of protective measures. Examples include coordinating with other Federal and State agencies and the private sector to: (1) ensure the detection of weapons of mass destruction material is considered in the development of protection plans; (2) disrupt attack planning by taking low cost actions that make information collection and surveillance difficult for terrorists; (3) defend the most at risk critical infrastructure facilities and key assets throughout the country above the level of security associated with industry best practices; and (4) develop a nationally-integrated bombing response capability similar to that of the United Kingdom. DHS funding in these areas focuses on high value, high probability targets and will take the form of “joint ventures” with State and local governments, regional alliances, and the private sector.
- Cyberspace Security.*—Consistent with the Homeland Security Act and the National Strategy to Secure Cyberspace, a key element of infrastructure protection, both in the public and private sectors, is to ensure the continued healthy functioning of cyberspace, which includes the cyber infrastructure and the cyber dependencies in the critical infrastructure sectors. The IAIP Directorate recognizes that cyberspace provides a connecting linkage within and among many infrastructure sectors and the consequences of a cyber attack could cascade within and across multiple infrastructures. The result could be widespread disruption of essential services, damaging our national economy, and imperiling public safety and national security. The budget request supports efforts to capitalize on existing capabilities of the Directorate, and investing in new capabilities to monitor, predict, and prevent cyber attacks and to minimize the damage from and efficiently recover from attacks. As the manager responsible for a national cyber security program, the IAIP Directorate provides direct funding to support: (1) creating a national cyberspace security threat and vulnerability reduction program that includes a methodology for conducting national cyber threat and vulnerability risk assessments; (2) strengthening a national cyberspace security readiness system to include a public-private architecture for rapidly responding to and quickly disseminating information about national-level cyber incidents—including the Cyber Alert Warning System; (3) expanding and completing the warning and information network to support crisis management during cyber and physical events; (4) implementing a national cyberspace security awareness and training program; (5) developing capabilities to secure the United States Government in cyberspace that include guidelines for improving security requirements in government procurements; (6) strengthening the framework for national security international cyberspace security cooperation that focuses on strengthening international cyber security coordination and; (7) the Global Early Warning Information System, which monitors the worldwide health of the Internet through use of multiple data sources, tools, and knowledge management to provide early warning of cyber attacks.
- Protection Standards and Performance Metrics.*—Working in collaboration with the National Institute of Standards and Technology as appropriate, the IAIP Directorate is developing objective data for systems protection standards and performance measures. Several sectors currently use threat-based exercise ap-

proaches to validate key elements of their protection efforts. The budget request in this area will focus on continually improving and validating sector plans and protective programs and providing training and education programs for public and private sector owners and operators of critical infrastructure and/or key assets.

Outreach and Partnership (\$40.829 Million)

The private sector and State and local government own and operate more than 85 percent of the Nation's critical infrastructures and key assets. Consequently, public-private cooperation is paramount, and without such partnerships, many of our Nation's infrastructures and assets could be more susceptible to terrorist attack. The IAIP Directorate is responsible for cultivating an environment conducive for public and private partnerships, developing strategic relationships underlying those partnerships, and coordinating and supporting the development of partnerships between the Directorate and State and local government, private industry, and international communities for national planning, outreach and awareness, information sharing, and protective actions.

The fiscal year 2005 President's Budget requests \$40.829 million to build and maintain a sound partnership foundation. It is imperative that the Department is familiar with the issues confronting the private sector, State and local governments, Federal sector specific agencies for critical infrastructure, and our international partners. Specifically, strong relationships must be maintained with the following communities of interest:

- State and Local Governments.*—Establishing and maintaining effective working relationships with State and local officials is a fundamental part of the DHS mission to effectively share information at unprecedented levels. IAIP is working with DHS' Office of State and Local Government Coordination to assess the information sharing and dissemination capabilities that exist nationwide in order to leverage existing capabilities and supplement capacity where needed.
- Private Sector.*—The Private Sector is another key partner in developing a nationwide planning, risk assessment, protective action, and information sharing strategy. Engaging the business community and making a business case for investment in protective and remedial strategies is key to our success.
- Academia.*—DHS will continue to develop, coordinate, and support partnerships with academic and other educational institutions. These partnerships will encourage and coordinate academic and other workforce development to assure availability of quality IT security professionals, and encourage curriculum development to integrate critical infrastructure protection (security) as normal elements of professional education.
- Advisory Bodies.*—DHS will also provide support to Presidential advisory bodies and cross-sector partnerships (including the National Infrastructure Advisory Council and the Partnership for Critical Infrastructure Security.)
- International.*—This funding will also support and enhance partnerships with the international community, working with and through DHS Office of International Affairs and the State Department, collaborating with the United States State Department on infrastructure protection activities. This includes bilateral discussions and activities on risk assessment and protective actions, information sharing, exercises and training. Of particular focus is the IAIP component of the Smart Borders implementation with Canada and Mexico. We will continue our role as the lead Federal Agency Role for the Information and Telecommunications Sectors. The Directorate will continue to partner with representatives from those industries composing the Information and Telecommunications sector and to educate members of the sector, develop effective practices, develop and implement intra-sector and cross-sector risk assessments, and work with other sectors on identifying and addressing risks associated with interdependencies.
- Cyber.*—We will expand the platform established by the Cyber Alert Warning System to include awareness and education programs for home users of computers and computer professionals in partnership with other Federal agencies and industry. Additionally, within private industry, our partnership and outreach efforts will involve the engagement of risk management and business educational groups to implement strategies to elevate senior management understanding of the importance of investment in cyber security.

National Communications System (\$140.754 Million)

The national telecommunications infrastructure supports multiple mission-critical national security and emergency preparedness (NS/EP) communications for the Federal Government, State and local governments, and the private industry. The secu-

urity and availability of the telecommunications infrastructure is essential to ensuring a strong national, homeland, and economic security posture for the United States. The National Communications System (NCS) is assigned NS/EP telecommunications responsibilities through Executive Order 12472, Assignment of National Security and Emergency Telecommunications Functions, which include: administering the National Coordinating Center for Telecommunications to facilitate the initiation, coordination, restoration, and reconstitution of NS/EP telecommunications services or facilities under all crises and emergencies; developing and ensuring the implementation of plans and programs that support the viability of telecommunications infrastructure hardiness, redundancy, mobility, connectivity, and security; and serving as the focal point for joint industry-government and interagency NS/EP telecommunications planning and partnerships.

The fiscal year 2005 President's Budget requests \$140.754 million for the capabilities and analytic tools necessary to support the expansion of NS/EP telecommunications programs and activities. The fiscal year 2005 funding level ensures a continuation of the NCS mission and legacy NS/EP telecommunications programs and assets. Specifically, the fiscal year 2005 budget request for the NCS is divided into four areas:

- Industry-Government and Interagency Processes.*—The NCS has cultivated and expanded its relationships with the telecommunications industry and other Federal agencies to promote joint planning, operational activities, coordination, and information sharing. The primary industry partnership is the President's National Security Telecommunications Advisory Committee (NSTAC), which is comprised of 30 industry leaders representing various elements of the telecommunications industry. The NSTAC and its subordinate body, the Industry Executive Subcommittee (IES), provides industry-based analyses and perspectives on a wide range of NS/EP telecommunications issues and provides policy recommendations to the President for mitigating vulnerabilities in the national telecommunications infrastructure. Paralleling this industry relationship is the interagency process involving the NCS Committee of Principals and its subordinate body, the Council on Representatives, which facilitate the NS/EP telecommunications activities of the 23 Federal agencies constituting the NCS.
- Critical Infrastructure Protection Programs.*—Leveraging the industry relationships described above, the NCS manages several network security and CIP-related programs, including: (1) the National Communications Center (NCC), a joint industry- and Government-staffed organization collocated within the NCS and serves as the operational focal point for the coordination, restoration, and reconstitution of NS/EP telecommunications services and facilities; (2) the Telecommunications Information Sharing and Analysis Center, which is the focal point for the generation, compilation, and sharing of cyber warning information among the telecommunications industry; (3) the Government and National Security Telecommunications Advisory Committee Network Security Information Exchanges (NSIEs), which meet regularly and share information on the threats to, vulnerabilities of, and incidents affecting the systems comprising the public network; (4) the Critical Infrastructure Warning Information Network (CWIN), which is designed to facilitate the dissemination of information and warnings in the event of a cyber attack; (5) Training and Exercises, which helps ensure the readiness and availability of qualified staff to perform the operational duties of the NCS associated with Emergency Support Function #2—Telecommunications of the Federal Response Plan; (6) Operational Analysis, which develops and implements tools and capabilities to conduct analyses and assessments of the national telecommunications infrastructure and its impact on NS/EP services; (7) NCS also supports the Global Early Warning Information System, which monitors the worldwide Internet health through use of multiple data sources, tools, and knowledge management to provide early warning of cyber attacks, (8) Shared Resources (SHARES) High Frequency (HF) Radio Program, developed by the NCS and in continuous operation since being approved by the Executive Office of the President in the NCS Directive 3-3 of January 1989. The SHARES program makes use of the combined resources and capabilities of existing Federal and federally affiliated HF radio stations on a shared, interoperable basis to provide critical backup communications during emergencies to support national security and emergency preparedness (NS/EP) requirements.
- Priority Telecommunications Programs.*—The NCS is continuing a diverse set of mature and evolving programs designed to ensure priority use of telecommunications services by NS/EP users during times of national crisis. The more mature services—including the Government Emergency Telecommunications Service (GETS) and the Telecommunications Service Priority (TSP)—were instrumental in the response to the September 11th attacks. Fiscal year 2005 funding

enhances these programs and supports the development of the Wireless Priority Service (WPS) program and upgrade to the Special Routing Arrangement Service (SRAS). Specifically, priority service programs include: (1) GETS, which offers nationwide priority voice and low-speed data service during an emergency or crisis situation; (2) WPS, which provides a nationwide priority cellular service to key NS/EP users, including individuals from Federal, State and local governments and the private sector; (3) TSP, which provides the administrative and operational framework for priority provisioning and restoration of critical NS/EP telecommunications services; (4) SRAS, which is a variant of GETS to support the Continuity of Government (COG) program including the re-engineering of SRAS in the AT&T network and development of SRAS capabilities in the MCI and Sprint networks, and; (5) the Alerting and Coordination Network (ACN) which is an NCS program that provides dedicated communications between selected critical government and telecommunications industry operations centers.

—*Programs to Study and Enhance Telecommunications Infrastructure Resiliency.*—The NCS administers and funds a number of programs focusing on telecommunications network resiliency, security, performance, and vulnerabilities, including: (1) the Network Design and Analysis Center, which is a set of tools, data sets, and methodologies comprising the Nation's leading commercial communications network modeling and analysis capability that allows the NCS to analyze the national telecommunications and Internet infrastructures; (2) the NS/EP Standards program, which works closely with the telecommunications industry to incorporate NS/EP requirements in commercial standards and participates in national and international telecommunications standards bodies; (3) the Converged Networks Program, which investigates vulnerabilities and mitigation approaches in future technologies and networks (specifically Internet Protocol-based networks); (4) the Technology and Assessment Laboratory, which provides the ability to evaluate penetration testing software, modeling tools, various operating systems and protocols, hardware configurations, and network vulnerabilities, and; (5) the Routing Diversity effort, which is developing a communications routing diversity methodology to analyze a facility's level of routing diversity and is evaluating alternative technologies which can provide route diversity, and (6) the NCS, through various associations and other activities is involved in a variety of International Activities (NATO, CCPC, CEPTAC, and Hotline) which provides technical subject matter expertise, guidance, and coordination on CIP issues affecting the telecommunications infrastructure in numerous international forums on behalf of the United States Government.

Competitive Analysis and Evaluation (\$18.868 Million)

The Competitive Analysis and Evaluation program ensures that IAIP products and services are tested, accurate, based on sound assumptions and data, and ultimately, offer the highest quality, depth, and value to IAIP customers. The fiscal year 2005 President's Budget requests \$18.868 million to provide for the unbiased, objective analyses and evaluation of IAIP findings, assessments, and judgments through three functional areas: Risk Assessment Validation, Evaluation, and Exercises and Methodologies.

—*Risk Assessment Validation.*—Funding is used to establish and field physical and cyber target risk analysis teams that employ "red team" techniques to evaluate measures taken by other IAIP components to protect key assets and critical infrastructure. The red teams emulate terrorist doctrine, mindsets, and priorities and employ non-conventional strategies to test and evaluate IAIP planning assumptions.

—*Evaluation.*—Funding supports several initiatives, including the IAIP Product and Process Evaluation, which involves conducting independent, objective evaluations of IAIP products and processes and to assist IAIP divisions to develop products that offer value to IAIP customers. The second is IAIP Customer Satisfaction, which evaluates customer satisfaction with IAIP products and services to ensure they are responsive to current customer needs. Funding in this area provides for electronic and non-electronic feedback surveys, field visits, and conferences.

—*Exercises and Methodologies.*—Coordinate and manage interagency exercises and tabletops that test both DHS and IAIP policies, processes, procedures, capabilities, and areas of responsibilities. Participating in and conducting after action reviews of exercises provides invaluable experience and feedback related to capabilities, connectivity, and information sharing during a crisis event. Investment in this area informs the Department's decision as to where improvements are needed. This funding also supports examining and instituting advanced

methodologies such as alternate hypotheses, gaming, modeling, simulation, scenarios, and competitive analyses to ensure IAIP products are accurate, sophisticated, and of the highest quality and value to customers.

National Plans and Strategies (\$3.493 Million)

Critical to ongoing national efforts to protect and secure the homeland are updating, revisiting, coordinating the development, and monitoring the implementation of National Plans and Strategies. The fiscal year 2005 President's Budget requests \$3.493 million to support activities by coordinating, developing, and publishing contingency planning documents for critical infrastructures (as called for in the National Strategy to Secure Cyberspace), monitoring progress against those documents, and producing an annual report.

Homeland Security Operations Center (\$35.0 Million)

The HSOC maintains and shares domestic situational awareness; coordinates security operations; detects, prevents, and deters incidents; and facilitates the response and recovery for all critical incidents. The HSOC is the focal point for sharing information across all levels of government and the private sector.

The HSOC facilitates the flow of all-source information and develops products and services including: (1) the daily Homeland Security Situation Brief for the President, (2) reports and briefs to law enforcement, the Intelligence Community, other Federal and State agencies and industry partners, (3) warnings and alerts to individual responder agencies and the public as appropriate, and (4) coordinated response when crises do occur. The HSOC concept is to draw from the many distributed systems and centers that are currently dedicated to different missions and optimize their contribution to homeland security.

HSOC funding will help with the time efficiency of issuance of information and warning advisories through increased operations efficiency brought about by facility improvements.

New Programs

In the fiscal year 2005 IAIP budget, as a part of an interagency effort to improve the Federal Government's capability to rapidly identify and characterize a potential bioterrorist attack, the President request \$11 million for a new biosurveillance initiative. This increase provides for real-time integration of biosurveillance data harvested through the Centers for Disease Control (CDC), Food and Drug Administration (FDA), United States Department of Agriculture (USDA) and DHS Science and Technology (S&T) Directorate with terrorist threat information analyzed at IAIP. Currently, a finding from one source of surveillance exists in isolation from relevant surveillance from other sectors, making it difficult to verify the significance of that finding or to recommend appropriate steps for response. Integrating the information in IAIP, and analyzing it against the current threat picture will inform effective homeland security decision-making and speed response time to events.

This interagency initiative, includes DHS's ongoing BLOWWATCH environmental biodetection program, Health and Human Services' (HHS) proposed BIOSENSE program, HHS' and United States Department of Agriculture's (USDA) ongoing joint separate food security surveillance efforts, and USDA's agricultural surveillance efforts. This DHS-led effort will promote data sharing and joint analysis among these sectors at the local, State, and Federal levels and also will establish a comprehensive Federal-level multi-agency integration capability to rapidly compile these streams of data and preliminary analyses and integrate and analyze them with threat information

Conclusion

In summary, the fiscal year 2005 budget request provides the resources to enable the IAIP Directorate to manage and grow in its mission of securing the homeland. I look forward to working with you to accomplish the goals of this department and the IAIP directorate.

Mr. Chairman and Members of the Subcommittee, this concludes my prepared statement. I would be happy to answer any questions you may have at this time.

NATIONAL BIOLOGICAL SURVEILLANCE

Senator COCHRAN. Thank you, General Libutti.

Now, looking at the budget request, I noticed that in the case of the National biological-surveillance program, the budget proposes to establish a group lead by the Department of Homeland Security and including the Department of Health and Human Services, and

the Department of Agriculture, to create a National biological surveillance system. Funding for this initiative is \$279 million Government-wide. The Department of Homeland Security's request for this initiative is \$129 million for the roles carried out by these directorates that you manage.

Secretary Libutti, how will the Information Analysis and Infrastructure Protection Directorate work to coordinate its efforts with the Department of Health and Human Services and the Department of Agriculture to integrate biological surveillance data, and verify a chemical or biological attack?

General LIBUTTI. Thank you, sir.

Let me start by simply highlighting the IAIP funds and support of this inter-agency effort. And I will tell you that my partner sitting here with me, to my right, Dr. McQueary, is certainly a partner for me in this effort.

For us, it's about \$11 million. And you touched on a critical point. Our job in support of this major inter-agency effort is to work as a repository to gather the data heretofore across the Federal Government, which is not indeed gathered, and looked at it with a view towards providing situational awareness, and as an extension, actions that need to be taken by the Federal Government, and by extension to partners at the State and local level.

So the bottom line for me in terms of how we do this, is I do it in complete support and cooperation with Dr. McQueary, and in concert with other members of the inter-agency effort. The bottom line is it's about gathering the information or data in a collaborative way, and in a way that represents what is going on across the Federal Government.

Senator COCHRAN. What would happen to this initiative if funding is not provided to the Department of Agriculture or Department of Health and Human Services? Would there be a serious breakdown in the capabilities of our government to deal with these threats?

General LIBUTTI. My sense, sir, is that if there were indeed a breakdown, it wouldn't be in the execution piece of their mission or their responsibility. It would be more broadly speaking, in what we have all learned is very critical in this fight against terrorism, and that is to truly work in concert to look at the information or databases that are available and simply haven't been collected in a cohesive way. To look at them and to ask, what does that mean in terms of assessing the threat, assessing our own capability, and then taking appropriate action.

Certainly, the mission would still be accomplished, I simply think it would not be a wise move in terms of the greater value added when you look at all of this data, and then there is one person responsible for bringing it together.

ENVIRONMENTAL MONITORING

Senator COCHRAN. Secretary McQueary, your directorate's role in biological surveillance includes an increase of \$65 million to expand environmental monitoring activities in the cities determined to be at the highest risk of terrorist attack. Can you give us any further details about the chemical and biological warning activities that

are in place now, and what this increased funding will be used for if it is made available to you by the Congress?

Dr. MCQUEARY. The increased funding will permit us to increase the number of sensors in high-risk urban areas, to be able to make the biological detections using a system called BioWatch. That system has been in place since about a year ago in January, when we first began deploying those systems.

And of course, you know we work very closely with EPA, as well as Health and Human Services, in being able to do that work.

Senator COCHRAN. What do you think you will be able to accomplish if you get this increased funding, in terms of new advances or the development of new technologies or systems?

Dr. MCQUEARY. The \$65 million is to allow more deployments of the capabilities than we currently have, thereby increasing the number of monitoring stations in the various urban areas where we have these systems already deployed, as well as increasing the number of locations, city locations, if you will, where we have them deployed.

So it fundamentally gives us a better, real—not real time-but a better monitoring capability so that we can make a determination should there be a biological attack of some sort.

We have approximately, I would say, an average of ten sensors per geographical location. Now that is an estimate but I can give you precise numbers if you need them. With the increase we will effectively be able to double the number of sensors where we are and provide better coverage, if you will.

COUNTERMEASURES

Senator COCHRAN. There is also the BioShield initiative, which is involved in deploying countermeasures against biological terror attacks. How is the Science and Technology Directorate participating in the development of countermeasures?

Dr. MCQUEARY. Well, of course, the development of countermeasures is in our charter, and we work in the chemical, biological, radiological, nuclear, and high-explosives areas. So in each of those areas we have ongoing research being managed either in the national laboratories, or in private industry or universities, which are three components of the country's scientific support that we call upon regularly. So, we do have broad agency announcements that have been put out through the HSARPA organization, for chemical, and biological sensors, as well as in the radiological and nuclear area.

And, if I may, the primary focus in all of the sensor development is to do things faster. Because, for example, BioWatch, we do a sample every day, but it takes perhaps a day to be able to do the assays on that sample, and therefore there could be 48-hours. The ultimate system that we would someday want to get to, and, some of our research, I think will lead in that direction, is to be able to do the sampling at the site, be able to do the assays, and then telemetry the information from that site to a central command control area. They would be working, obviously, very closely with General Libutti's people to make a determination that something has happened, and therefore, corrective action would be taken.

Senator COCHRAN. Does this budget request include research and development of medical countermeasures across the agencies portfolios, or does the Science and Technology Directorate serve only in an advisory role?

Dr. MCQUEARY. The medical countermeasures is the responsibility of Health and Human Services. We serve in an advisory role in that area, and have people that meet regularly with people in Health and Human Services to discuss programs that should be implemented.

Senator COCHRAN. What assessments have been carried out by the Information Analysis and Infrastructure Protection Directorate of our vulnerability to biological attacks that will guide decisions regarding the investments that should be made to develop, produce and purchase vaccines or other medications for the Nation's biological defense.

General LIBUTTI. The work that we have done since I have been on board, since late June or early July, sir, has been to work with Dr. McQueary and his folks, conduct surveys and visits across the country to key high-threat areas, to get as smart as we can relative to the threats posed by the biological and chemical threats, and to conduct appropriate analysis including developing models to give us a strong indication of what the impact of such an attack would be.

We have recently developed a program that we have briefed to high officials in our government, in the Administration, that outlines across the board threats in aviation, transportation, and biological, and chemicals weapons. What we have developed is still a work in progress. But it is a good model. We've looked at the impact and consequences of various events particularly across major urban areas.

So those are the kinds of activities that we have been engaged in, in concert with Dr. McQueary and other members of the inter-agencies; specifically, Health and Human Services, CDC, and others who have a primary interest in the impact of such an attack.

INTEROPERABLE COMMUNICATIONS AND SAFECOM

Senator COCHRAN. Senator Byrd.

Senator BYRD. Thank you, Mr. Chairman.

Secretary Ridge has laid out the department's goals, and he stated that one of his highest priorities was interoperable communication and equipment. And he set a deadline of December 2004, for implementing a short-term solution, that will allow first responders to communicate with each other during a disaster. Dr. McQueary, your directorate is in charge of coordinating and promoting interoperable communications for public safety.

The President's budget proposes to eliminate funding in the Justice Department for interoperability grants. When my staff asked the Justice Department why the funds were dropped from the budget, my staff was told that interoperability is a Homeland Security responsibility. Yet the President's budget sets aside no funds for this purpose in the Department of Homeland Security budget. So I ask, can you explain the short-term solution and why no funds are requested to address this problem?

Dr. MCQUEARY. We actually do have funds requested to support the SAFECOM program, which is the program for which the Science and Technology Directorate has direct responsibility.

Senator BYRD. How much is the request?

Dr. MCQUEARY. I believe, sir, \$20—if I am not mistaken, its \$22 million. I'll check behind me, and make sure I give you the correct number. But I believe it's \$22 million for that effort.

And what we expect to come out of that effort, as Secretary Ridge had indicated, is a set of standards that State and local, can use to acquire equipment, and to provided interoperability on what we're referring to as the penultimate solution, because what we will be providing is not the ultimate solution in interoperability. I will try to be precise in what I mean by that.

There are technical capabilities today that exist in some companies. For example, if you think of a point electronic box, a box that can receive signals from many different types of radios, and that box can in effect convert signals from one radio into a protocol or a format that would be needed by another radio it is trying to talk to in order to permit those two to be able to have a communication. And, similarly, you can create conference calls, if that were the objective. Obviously, there are limits to the number of possibilities of different kinds that can be implemented.

The ultimate solution, I believe, will be to move into software defined radios, and a considerable amount of research work has gone on in that area. That would be a system in which new radios, as they are purchased, would permit people to communicate with one another based upon the radio itself being able to recognize the different types of communication protocols and accomplish that.

Senator BYRD. The SAFECOM money is not money for State and local governments.

Dr. MCQUEARY. That's—

Senator BYRD. SAFECOM is for standards setting. To actually fix the problem, State and local governments need money to buy the interoperability equipment.

Dr. MCQUEARY. Excuse me.

Senator BYRD. Yes.

Dr. MCQUEARY. I did not mean to imply that the \$22 million that we have in our budget is to be used to purchase equipment. It is indeed the necessary effort to establish the standards. Of course, the State and locals will have access to grant money that will be provided by the Office of Domestic Preparedness. And what we will do, and have already done in some cases, is provide guiding standards by which we would expect them to purchase new equipment in the expenditure of that money. We see that as the vehicle to permit State and locals to be able to transition into having more interoperable capability.

Senator BYRD. The President is proposing a cut of over \$700 million of first responder programs in the Department, and a cut of \$1.5 billion for first responders government wide.

The interoperability problem is yet another reason why we should not be cutting funding to first responders. How does the Department justify cutting first responder grants when the short term solution that the Secretary announced will cost several million dollars to implement?

Dr. MCQUEARY. If you're proposing that to me, sir, I was not a participant in that, and therefore, I am not in any position to answer the question, but I am sure that my people will be pleased to provide an answer to the question that you proposed.

[The information follows:]

JUSTIFICATION FOR CUTTING FIRST RESPONDER GRANTS

The President's fiscal year 2005 request includes more than \$3.5 billion to support ODP programs and activities. This represents a \$3.3 million increase over the Fiscal year 2004 request. The fiscal year 2005 request includes funds to continue the Homeland Security Grant Program which includes the State Homeland Security Program at \$1.4 billion; the Law Enforcement Terrorism Prevention Program at \$500 million; and the Citizen Corps Program at \$50 million. Funds are also provided for the continuation of the Urban Areas Security Initiative at \$1.4 billion; the Fire Act Program at \$500 million; the Emergency Management Performance Grants at \$170 million; as well as for ODP's training, exercise, and technical assistance efforts.

The continuation of these efforts, and the \$3.3 million increase in ODP's overall request, coupled with the President's request for a 10 percent increase in funding for DHS as a whole, provides ODP, and the entire Department, with the resources we require to help secure the Nation from acts of terrorism. The Administration and Department remain committed to providing our Nation's emergency prevention and response community the resources they need to continue to secure our Nation from future acts of terrorism.

UNIVERSITY PROGRAMS

Senator BYRD. Your budget request includes a \$38.8 million reduction for Homeland Security University and Fellowship Programs. In fiscal year 2004, this subcommittee provided \$69 million for this program, \$60 million more than the President requested. The subcommittee expects the academic community to play a major role in identifying and solving problems facing the homeland.

The White House has criticized Congress for earmarking funds for Science and Technology, and so this subcommittee decided not to earmark funds last year. Instead of reinforcing this decision, the President is proposing to cut university research by over 50 percent. Could you tell the subcommittee what the rationale may be for such a drastic cut to this program in fiscal year 2005?

Dr. MCQUEARY. This is an area in which I can assure you we had considerable internal debate and discussion. I would have to hasten to say, sir, that at some point we all work for someone and it was time for me to salute and say, yes, sir, I will try to do as much as we possibly can with the proposed amount of budget, and that is what we will do.

Senator BYRD. Your budget justification notes that three Homeland Centers of Excellence will be selected by the end of fiscal year 2004. How does this funding reduction affect your ability to select other university centers of excellence.

Dr. MCQUEARY. First, the \$30 million that's proposed is ample funding to support three University Centers of Excellence. We have, of course, selected one. And we plan to select two more this fiscal year. In fact, the necessary activity is well underway in order to accomplish that.

We fund the University Centers about \$5 million each, minus a little bit of overhead associated with managing that process. The balance of \$15 million is completely adequate to support not only

the hundred fellows and scholars that we have already approved. But also to add another hundred to that.

In summary, \$30 million supports three Centers, as well as 200 scholars and Fellows.

Senator BYRD. So you're saying, are you, that there will be two additional centers selected at the President's funding level?

Dr. MCQUEARY. I am sorry, sir.

Senator BYRD. Are you saying that there will be two additional centers selected at the President's funding level?

Dr. MCQUEARY. Yes, sir, there will be two additional, bringing us to a total of three. One is in animal diseases. The other is in post-harvest food safety.

CHEMICAL DETECTORS

Senator BYRD. In your written statement you list as an accomplishment of your directorate that you worked with the D.C. Metro System to deploy chemical detectors in the D.C. subway system. This is an excellent system to give Metro the capacity to immediately determine that the subway has been exposed to a chemical agent, so it knows how to effectively respond to the attack.

I understand that this system is now in operation and you view it as an accomplishment. After the attacks of 9/11, the Senate approved \$15 million for this pilot project. This funding was included at Congress's initiative, it was not requested by the President. In fact, the White House specifically objected to this funding, describing it as excessive.

Is there any funding in the President's request to either complete the D.C. chemical detector system, or to take advantage of the lessons learned from this pilot program to deploy the chemical detectors in other large subway systems around the country?

Dr. MCQUEARY. Well, at this time we have proven the concept of operation for that system, and it is something we are extremely proud to have been a part of, I can assure you. So, I compliment the Congress on appropriating the funding necessary to get it launched.

We do have the measurement system, both chemical measurement as well as video capability, tied into a central control station in downtown D.C., as you probably know, I am sure you know. We view it as a responsibility of Washington, D.C. to carry the program forward, for example, if there is a need or desire to expand to more stations within the Washington, D.C. area.

MANPADS SURFACE TO AIR MISSILE COUNTER MEASURES

Senator BYRD. Your budget includes \$61 million to determine whether a viable technology exists to address the threat shoulder-fired missiles pose to commercial aircraft. This funding request followed \$60 million approved by Congress in fiscal year 2004. The details of this threat are well documented. The Congressional Research Service estimates there are as many as 700,000 of these missiles globally. Some of which are on the black market, selling as low as \$5,000 apiece.

CRS also estimates that there have been 29 instances in which civilian planes have been hit by shoulder-fired missiles, none of which occurred in the United States.

However, in May 2002, the FBI warned law enforcement agencies to be alert to the potential use of surface-to-air missiles against U.S. aircraft. If such a missile was fired at a commercial aircraft here in the United States, it would wreak havoc on our economy.

How soon do you believe that we can begin to outfit commercial aircraft with a system to counter surface-to-air missiles?

Dr. MCQUEARY. I believe that we expect by the end of calendar year 2005 the Administration and the Congress will be in a position to have scientific information from which to make a decision as to whether we should outfit planes, commercial aircraft, in this country.

Science and Technology, as an organization, will not be recommending one way or the other. Rather, that is a decision for the Administration and the Congress to make, we believe.

Senator BYRD. How realistic is it to convert to existing technology on military aircraft to our commercial fleet?

Dr. MCQUEARY. We believe that it is in the category of, what I would call, an engineering problem, rather than needing a scientific breakthrough in order to do this. There are really two or three issues that drive the commercial airline fleet. Of course, one is that certifications necessary to get approval to put anything on an aircraft is perhaps more stringent for commercial aircraft.

Also anything we do to an aircraft that would add air drag will increase fuel costs, and so there are multiple issues to be dealt with as one decides which technology would be appropriate. Regarding the technologies themselves, we do believe that it is eminently feasible to put them on commercial aircraft. And, we have three contractors that are in the early stages of studies that will lead to a down selection of one or two contractors to go into the development of such a system.

The other important factor is that reliability must be such that we can afford to have them on the planes. The military can actually carry its support system with it wherever the planes fly. But, if you consider all of the airports into which our planes go, just in this country alone, the idea of trying to have a support system at each one would be extremely expensive.

So the reliability of the systems need to be greater than what we are seeing with the military versions right now.

Senator BYRD. Do I have time for one more?

Senator COCHRAN. Senator Stevens has come in and we want to include him.

Senator BYRD. I shall desist.

Senator COCHRAN. Senator Stevens.

TSA DETECTION SYSTEMS

Senator STEVENS. Thank you very much.

I was enjoying the Senator's questions, as a matter of fact. I, gentlemen, have spent quite a bit of time with the aviation community trying to figure out where we're going in terms of some of the homeland security activities. And, I am impressed with comments that I have received from many of them that our systems are designed to deal with metal and not with substances. How would you answer that?

Dr. MCQUEARY. Our systems are designed to deal with—

Senator STEVENS. Metals rather than substances.

Dr. MCQUEARY. Metals rather than . . .? I'm afraid I don't understand the question, sir.

Senator STEVENS. Well, we're looking for guns, we're looking for knives, we're not looking for chemicals, we're not looking for biological weapons. We're zeroing in on what was used in 9/11 and not what the terrorists might be using in the future. Is that correct?

Dr. MCQUEARY. Now, I understand the question. Within the Science and Technology Directorate we do have some research work that we're funding this year to be able to make detections of explosive devices at range, if you will. This is in the very early stages, and I would not for a moment try to tell you that I think that we have a solution to that problem.

The Israelis have, of course, worked on this in great detail. We have had many interactions with them. It's a hard problem, but it is an area which we think is important towards being able to do the things necessary to make the airports, airlines and travel safer. It is a very important area.

Senator STEVENS. Well, over the past recess, I went through major airports, and I asked to be shown the TSA systems. And, I must say they are very impressive systems, but all of them are designed for what I said, to locate knives, to locate metals that might be in the baggage. Are we looking towards trying to ascertain the presence of chemical substances, bacterial substances, and explosive substances?

Dr. MCQUEARY. I will tell you, the area where I do not believe we have a satisfactory answer to in the bacterial area. It's very complex, very difficult, to deal with what a person can do to bring something in a handkerchief into the country. It would be very, very difficult to detect a bacterial substance, unless one were to get into some sort of invasive type of measurement system. So far, we have not chosen to get into that level. We as a country, have not chosen to go that far.

In chemicals, there are many different types of detectors that can indeed detect chemical components that would make up explosive systems or any kind of liquids that you might have. But you have to be able to get a sufficient signal, if you will, a sufficient amount of the chemical being put forth into the air so that it could be detected, unless we go to some kind of invasive system. And right now, our focus is on what we might be able to pick up from the air, if you will, the general air surrounding a passenger in that area.

Senator STEVENS. Well, Doctor what about the President's—

Dr. MCQUEARY. We are not ready to—I'm sorry.

Senator STEVENS. I beg your pardon.

Dr. MCQUEARY. Please continue.

Senator STEVENS. What about the presence of detonators? We're watching daily in Iraq bombs go off by someone dialing a cell phone.

Dr. MCQUEARY. Right.

Senator STEVENS. And alerting, you know, energizing a detonator. Are we trying to discover the presence of detonators in baggage?

Dr. MCQUEARY. I can't answer the question. I don't know off hand—I simply don't know. I should know the answer, but on that particular question, I don't know. I will be happy to look into it and find out exactly what we are doing for you.

[The information follows:]

DISCOVERING PRESENCE OF DETONATORS IN BAGGAGE

Reliable detection of detonators in baggage is important to the security of the transportation infrastructure. The responsibility for this security measure currently remains with the Transportation Security Administration. Additional information can be provided in a classified briefing.

Senator STEVENS. Alright.

RESEARCH AND DEVELOPMENT CONSOLIDATION

Let me shift to the Coast Guard, if I may. Are any one of you involved in the changes that are taking place in research and development funding. That's in the Science and Technology Directorate.

Dr. MCQUEARY. That's right.

Senator STEVENS. That's yours, is it Doctor?

Dr. MCQUEARY. Yes, sir.

Senator STEVENS. When we approved the transfer of the Coast Guard to the new Homeland Security Department, it was my understanding, and I think that it was in the basic law and in the report, that the department was to be left as a complete unit. I am informed now that the budget proposes to transfer the research and development funding in units of the Coast Guard to your directorate. Is that right?

Dr. MCQUEARY. That is correct. But, I need to be precise on what we mean by transfer. That unit will never lose its close ties with its parent organization. We will assume research and development oversight for it.

As you are probably aware, the Congress actually cut the research and development budget for the Coast Guard laboratory last year. So they entered this year with no money other than support for the people that are in that laboratory. They have had no research and development program in this fiscal year. We do have money in our Science and Technology budget for fiscal year 2005 to support the Coast Guard, not only the people at the laboratory, but also a modest research and development program.

SHIFT OF \$13.5 MILLION FROM THE COAST GUARD TO THE SCIENCE AND TECHNOLOGY DIRECTORATE

Senator STEVENS. My information was that the budget proposes to shift \$13.5 million from the Coast Guard to your directorate. Is that wrong?

Dr. MCQUEARY. No, that's not incorrect. The \$13.5 million is basically the operational costs for the labs that are in Connecticut. And we're putting in another \$5 million for research and development work.

Senator STEVENS. Are you taking over direction of it, and taking it from the Coast Guard?

Dr. MCQUEARY. That's harsher language than I would choose to use.

Senator STEVENS. The language. The legislation is very harsh. I drew it.

Dr. MCQUEARY. Okay. We have responsibility, we had responsibility in the Science and Technology Directorate to advise and direct the Coast Guard on what scientific work they needed. However, I would say directly, that in order to accomplish the determination of what we must do, we have Coast Guard people on our staff, we have a Coast Guard Captain who is in residence with my Science and Technology group. His job is to make sure that we're representing the needs of the Coast Guard in the scientific work that we undertake. And that's the same thing we do for each and every one of the operational units within the Department of Homeland Security.

We're not an independent island on research and development. We're a service organization intended to provide the very best science and technology to these operational units which stand at the ready each and everyday to do the job the Department of Homeland Security has to do.

Senator STEVENS. Well, it's a technicality I imagine, but when Congress declares war, the Coast Guard becomes a part of the Department of Defense.

Dr. MCQUEARY. Right.

Senator STEVENS. You're familiar with that?

Dr. MCQUEARY. Yes, sir.

Senator STEVENS. The legislation we passed to authorize the transfer of the Coast Guard to the Department of Homeland Security was done in a fashion so that, if that transfer to the Department of Defense was triggered, it would be a whole unit.

It appears to me that slowly but surely you're taking away from the Coast Guard the things that make it a whole unit, namely research and development.

Dr. MCQUEARY. I spent my entire career in research and development, and my experience tells me that small pockets of research and development can never be as effective as being a part of a larger research and development organization. We believe that by transferring the Coast Guard's research and development into the Science and Technology Directorate, and giving them more day-to-day interaction with the scientific work that is going on, that we will actually end up doing a better job, not only for the department, but also for the Coast Guard itself.

Senator STEVENS. Are you prepared to do that for the Department of Defense when it becomes a part of the Department of Defense?

Dr. MCQUEARY. I—

Senator STEVENS. I don't think you get my point. You have no authority to do that.

Dr. MCQUEARY. We have—

Senator STEVENS. I would urge you to check with your legal department and determine what authority you have to transfer anything from the Department of Defense, from the Coast Guard, without our approval.

Dr. MCQUEARY. Well, I am sure that if we don't have the authority to do it, we do not propose to do it without your approval, if that's the case.

Senator STEVENS. Sometimes people are ignorant of the law.

Dr. MCQUEARY. Well, that could very well be the case here, too.

Senator STEVENS. Well, I don't think.

Dr. MCQUEARY. But I can assure you that there is no intention—

Senator STEVENS. I don't mean to be abrupt with you Doctor, but I do believe that it is essential that if and when the Coast Guard becomes a part of the Department of Defense, it be a total unit.

Dr. MCQUEARY. Yes.

Senator STEVENS. An integral, operational unit that is just transferred and not leaving portions of it somewhere else. That was the debate that we had, and I hope that we will pursue that and you will take a look at it for us.

Now, let me ask you—

Dr. MCQUEARY. I will do that.

UNIVERSITY PROGRAMS/ENERGY SECURITY

Senator STEVENS. One other thing if I may. Well two really. I see that you have got these Homeland Security Centers of Excellence, and I congratulate you. The Senator from West Virginia was talking about one in terms of the Center for Excellence with regard to food programs. And one, I understand, will be combating animal related agro-terrorism, and the other focuses on post-harvest food security.

What about energy production and energy security. Are you focusing on that?

Dr. MCQUEARY. For the areas of energy production and energy security is a combination of General Libutti and myself, as well as the Department of Energy. I believe one of the Homeland Security Presidential Directives clearly spells out that the Department of Energy has responsibility for energy. So the work that we do would be to work with General Libutti from an infrastructure protection standpoint. And, perhaps I would let him comment rather than be presumptive about saying what he would be doing.

Senator STEVENS. General, are you pursuing that?

General LIBUTTI. Sir, the effort that we make in the main, in terms of our mission profile, is the risk assessment vulnerability piece of any part, large or small, of the national infrastructure. So in terms of chemical site security surveys, we are working with our friends at the Nuclear Regulatory Commission, working with other members in the inter-agency, and our job remains principally to advise relative to the threat.

We recommend preventive actions in concert with the rest of the community, that ought to be taken immediately or that have a long-term proposition relative to protecting America. So, we're about the threat, vulnerability and risk assessment piece of all of these programs. And we share that information with my friend, Dr. McQueary, and other members of Health and Human Services, Center of Disease Control, the Department of Agriculture, or the Department of Energy.

So we're a player at the table. I might add, and this is not a marketing piece, but we are the newest members of the National Intelligence community, and we are full players. We have connected very well with all the major elements within the Federal Govern-

ment, as well as State and local communities that deal with information sharing, analysis, and simply stated the threat.

I tell you that just for a sense of what our directorate is all about and how we interact with other members of the intelligence community, including TTIC, CIA, and the FBI, who principally has responsibility on the law enforcement side.

Senator STEVENS. Thank you.

I will be delighted to try and understand what you just said. For instance, in terms of our oil pipeline, do you review that pipeline for threat?

General LIBUTTI. We do when we gleam specific intelligence from looking at all of the sources, which indicates that it is a target set. We absolutely look at it in the broader infrastructure requirements that bring us to a situation which causes us to look at it with other members of that community.

Senator STEVENS. And do you—

General LIBUTTI. And we do that across all of the infrastructure.

Senator STEVENS. Do you review the ports through which we import 57 percent of our oil?

General LIBUTTI. Again, we work in concert with our friends in the Coast Guard and in the industry, the container shipping folks, to look very hard at the threat and the risk associated with that threat, in a specific port, city, or State.

So the answer is, yes, sir, we do.

Senator STEVENS. Okay.

ENERGY SECURITY

Well, let me give you one that I think you ought to take a look at then. And the Department of Commerce can verify this.

By 2015, we will be importing 40 percent of our natural gas in the form of LNG. We do not have a LNG port in the United States. We have authorization. Years ago we passed legislation to have offshore ports, but none were ever built. I think that in your department you ought to be looking at the planning for the future, how are we going to ensure the security of that, and how will it be relevant to the importation of oil and other substances.

Should we separate those ports from existing ports by having them all come into one port? Obviously, that would increase the possibility of the threat.

But, I haven't heard anyone talk about planning for the national security, or homeland security on the access of natural gas in liquefied form.

General LIBUTTI. Sir, you're absolutely right. When that is teed up as a critical issue, and I think from your perspective we ought to be teeing it up right now, we would be very much involved in looking at that. Not from an engineering standpoint, or the physical lay-down standpoint, but from the threat perspective.

And you're absolutely right, we should be involved in that, and I will take your note back and we will take a look at it to see what we need to do right now.

Senator STEVENS. Don't put me down as an advocate, I would just assume bringing Alaska's gas down. But it seems that other gas is going to get here first, sir.

Thank you very much, Mr. Chairman.

Senator COCHRAN. Thank you, Senator Stevens.

UNIVERSITY PROGRAMS

Let me follow up with a comment about a question Senator Byrd asked on the Centers of Excellence, the university programs that we were talking about with Dr. McQueary.

Last year, we appropriated about \$69 million and it was intended to support these programs. Just because the Administration is requesting only half of that, \$39, \$30 million, doesn't mean that you shouldn't spend the \$69 already appropriated. There are provisions for deferring expenditures or rescinding expenditures, but there is no provision for not spending it.

So, what I am suggesting is that money is in the pipeline and it may very well support more than three university centers.

Dr. MCQUEARY. If I may, it will support more than three universities. And in fact, what we have determined already, sir, is that we can create five universities when we reach the limit of the money that you have authorized us in fiscal year 2004. But, when that is gone, we would be faced with having to cut back to the three.

I have asked for a plan already as to how we would implement a total of five, recognizing that we could be faced with having to eliminate two of those at the end of their 3-year period, which is what we're looking at right now.

Senator COCHRAN. Thank you.

NOAA WARNING ADVISORY SYSTEM

I am going to yield, again, for questions from Senator Stevens. And then we will go back to you, sir.

Senator STEVENS. If I may just ask one.

I forgot to ask a question about the NOAA Weather Radio. We asked that the Department prepare a report by December 15, of last year, on the use of NOAA Weather Radio as a component of a national warning system measure to expand consumer access to the warning systems in efforts to inform and educate the public about national security.

Currently we rely upon the radio for the old national warning system. We have tried to expand so that all forms of communication would receive the warning, particularly of a terrorist event. And all portions of the country could be alerted to that immediately. As I said, currently, that would only go out by radio, but it does not use NOAA Radio. NOAA Radio hooks into almost every radio station, television, and weather program that there is in the country. I particularly would favor some national legislation to mandate carrying such messages, or to include putting them into the internet directly. But, that hasn't been done yet.

However, we did ask for the NOAA Weather Radio to be used as a component of the warning system. Who is working on that in your Department?

Dr. MCQUEARY. Sir, I don't know.

General LIBUTTI. Sir, we have the lead to look at that in terms of how it fits into our broad responsibilities, as I outlined in my presentation of information sharing and alert advisory systems. So we are indeed looking at that, and that is still a work in progress.

Senator STEVENS. Well respectfully, General, we asked in 2002 for a report by December 15, 2003. When will we see your report?

General LIBUTTI. Sir, I will take that on board as an action and get back to you and your staff.

[The information follows:]

NOAA ALERT SYSTEM REPORT

The congressional report has been cleared by OMB and the Department. The report was approved for transmission to the Hill on May 28, 2004, and delivered on June 1, 2004.

Senator STEVENS. Thank you very much.

Thank you, Mr. Chairman.

Senator COCHRAN. Thank you, Senator.

Senator Byrd.

General LIBUTTI. If I may, sir, as a continuation, I will get back to you as soon as I can within the next couple of days. But a staff note to me reminds me that we were going to come to grips with your question very, very soon. And I will define what soon means when I respond to you.

Senator STEVENS. Thank you very much.

General LIBUTTI. Yes, sir.

CRITICAL INFRASTRUCTURE PROTECTION

Senator BYRD. Thank you, Mr. Chairman.

Last year, General Libutti, I asked Secretary Ridge about the role of the Federal Government in protecting chemical facilities from terrorist attack. He said that he believes chemical companies should be conducting their own assessments and paying for security improvements.

At the Secretary's budget hearing last month, Senator Murray asked Secretary Ridge about port security funding. And the Secretary again held the view that port owners should be responsible for security investments.

Now General Libutti, if you were the CEO of a chemical company, your highest priority would, probably be creating a quality product at a price that would create profits. If you were the director of a private port, your first priority would, in all likelihood, be that of maximizing the number of containers or passengers that would use the port.

And so with all due respect, I have very little confidence that chemical company CEOs or port directors would have defending against a terrorist attack at the top of their list of things to spend money on. Yet, the Department clearly believes that, when it comes to protecting our critical infrastructure the private sector should bear the financial burden.

Can you provide the subcommittee, today, with any benchmarks that you have established to show the private sector is making the necessary investments to secure our critical infrastructure and key assets?

General LIBUTTI. Sir, I appreciate the question because, like you, chemical site security for the Nation is a priority for IAIP and the Department. I would tell that I believe the right answer to how we move forward with our chemical site partners in the private sector,

the Federal Government, and my Directorate is the key word partnership.

I think the industry overall needs to belly-up to deal with improved security across their industry, especially in particularly high-threat areas. As a subset of that, I would emphasize the high-threat areas near large populated areas across the country.

Over the last several months we have conducted site surveys where folks from my office have visited top priority target sets involving the chemical site areas. We have worked with them, and we have seen them demonstrate a great spirit of cooperation in dealing with assessing the risks of their facilities, and taking actions to improve the readiness of those facilities, in terms of both preventative and recovery activities.

I cannot, sir, tell you the kind of money that they have, as an industry, put toward this effort. I will look into that and provide you our best estimate and judgments. But I cannot answer that question right now.

I think what is important, I might add to share with you sir, is that during the visits we worked to improve readiness, we highlighted protective measures, standoff distances, buffer zones, cameras, and command and control systems, all which they took on in a very positive way.

We have also sent out to all sites, not just the sites that we have visited, several different documents or what I would call aids in improving their readiness. We have sent out the following: characteristics and common vulnerabilities of chemical sites/facilities; potential indicators of terrorists attack activities for chemical facilities; and buffer zone protection planning templates for chemical facilities.

We have really looked at this in the same way that you have. This is a critical priority because it is a critical target site for potential terrorist attacks.

We have looked at the highest areas of concern because of the relative impact on the community, if indeed an event occurred. And we have a plan over the next year to look at an additional 360 sites or facilities across the country. I might also add that the focus is to look at this in a realistic way not in terms of eliminating all threats, but dealing with this based on what I call risk management across our country. That is to say that we have to establish priorities, and indeed, the Federal Government in concert with our friends in the community have to attack this thing on a single front.

I didn't mean to be so long winded, but that captures my concerns and the actions we're taking.

Senator BYRD. Well General, could you provide the subcommittee with any benchmarks that you have established to show that the private sector is indeed making the necessary investments to secure our critical infrastructure and key assets?

In other words, Secretary Ridge says, it's up to the private sector. So have you established any benchmarks that show that the private sector is indeed making the necessary investments to secure this critical infrastructure and key asset?

General LIBUTTI. Sir, as I indicated earlier in my first statement of my presentation here, I don't have specifics relative to the finan-

cial investments. If my staff has those, I'll provide them as quickly as possible. If not, we will do the research to get that to you.

I would say, just spinning off the Secretary's comment, and based on my experience, since I have been on board from late June or early July, I have seen not only a willingness and spirit of cooperation, but an understanding on the part of the chemical site industry and other industries, which we call key critical industries, a willingness to move out smartly, to do what needs to be done to protect their equities, to improve the security to their physical sites, etcetera, etcetera.

So the attitude is there. We will continue to capitalize on that, and I will get you the information you have asked for, sir.

[The information follows:]

SECURING OUR CRITICAL INFRASTRUCTURE AND KEY ASSETS

As part of a wide effort to facilitate rather than mandate, DHS continues its effort to develop "best practices" for industry by working with the private sector and professional associations. DHS believes that the private sector, which controls over 85 percent of the nation's critical infrastructure and key assets (CI/KA), must be involved in setting national protection standards. By partnering with associations and groups, DHS plans to create realistic, proactive protection practices to bolster the physical hardening of the nation's CI/KA.

One example of DHS working closely with industry is the ASME Guidance on Risk Analysis and Management for Critical Asset Protection. This important effort is intended to demonstrate that industry can not only provide DHS leadership with information, but can also help create industry-based guidance for risk analysis and risk management. This document will establish common terminology and a common basis for reporting the results of risk studies, helping the protection community and the private sector streamline and standardize risk analysis reporting. Such standardization provides government agencies and private industry a framework from which to collect, report, and respond to potential terrorist threats.

The ASME effort highlights how DHS is working closely with the private sector to develop baseline best practices and protective measures. Our plan is for these guidelines to mature into sector-wide protection standards that will be adopted industry-wide. The initial phase of the ASME effort is to focus on Nuclear Power Plants, Spent Nuclear Facilities, Chemical Plants, Petroleum Refineries; LNG Storage Facilities, Subway Systems (including bridges and tunnels), Railroad Systems (including bridges and tunnels) and Highway Systems (including bridges and tunnels). Depending on the success of the initial effort, it may be expanded to encompass other infrastructure categories.

Another important DHS initiative to assist private industry in the protection of their facilities is the preparation and distribution of analytic products such as Characteristics and Common Vulnerabilities and Potential Indicators of Terrorist Activities reports. These products identify those vulnerabilities and threat indicators that are sector-specific. Such information, when used by industry, allows intelligent investments to be made to eliminate or mitigate specific vulnerabilities. Furthermore, DHS is in the process of fielding a network of Protective Security Advisors and establishing regional offices that will assist State and local governments, as well as the private sector, in their protective planning efforts.

Senator BYRD. Alright.

As I said in my opening statement I will be asking the General Accounting Office to conduct an independent review of the private sector's role in securing our critical infrastructure.

It will be essential in assessing the need for investments, for Federal investments, to secure our critical infrastructure. So, it will be essential for Congress to have measurable benchmarks of private sector investments in such infrastructure, such as investments in chemical facilities, port security, and cyber security.

Do you agree that having this information would be useful to determine if the private sector is meeting its obligation to protect our critical infrastructure?

General LIBUTTI. I can't see how it wouldn't be supportive and an indicator of their commitment. But as I said earlier, this is a partnership in my opinion, sir. So the Federal Government needs to provide advice, and education, in concert with Dr. McQueary and his folks and other members of the inter-agency, and share with them best practices, and cutting-edge technology. That's all part of this movement forward. So I don't see how that could hurt.

I would be concerned if it became a weapon to be held up against them. Again, I think as we move forward we need to determine the right balance. But, I hear you loud and clear, and we will do our homework and get back to you, sir.

TERRORIST THREAT INTEGRATION CENTER (TTIC)

Senator BYRD. Alright, General.

One of the most important issues affecting the public's assessment of the Department of Homeland Security performance involves its record of sharing Homeland Security threat information with other Federal agencies, as well as with State and local governments, the private sector and the public.

The Gilmore Commission, in its December 15 report, noted that the Department of Homeland Security had "little power and capability to do this." In fact, the Commission concluded that the Department of Homeland Security faces significant competition from other agencies in disseminating information to State and local authorities, the private sector and other areas.

Part of the problem, the panel said, is that the CIA was granted control over the Terrorist Threat Information Center, or better known as TTIC, which opened in May as a central repository for information from the CIA, the Department of Defense, the FBI, the Department of Homeland Security, and other intelligence agencies.

But Congress, in writing the Homeland Security Act, envisioned giving the Department of Homeland Security the role of collecting, analyzing and sharing intelligence information. Putting TTIC at the CIA, the Gilmore Commission said, has largely sidelined the Department of Homeland Security and left it with a paucity—that's a good word—and left it with a paucity of competent intelligence analysts.

While intelligence professionals have been much more willing to go to the CIA, the Department of Justice, the Department of Defense, or the State Department, this seems to have caused confusion at all levels of government regarding the respective roles of the TTIC and the Department of Homeland Security.

CONCERN REGARDING TTIC BEING UNDER THE LEADERSHIP OF THE
CIA

Could you explain please, how it came about that the CIA was given the leadership of this intelligence function. And second, how it is that our homeland is made more secure by having such a confusing hierarchy of intelligence sharing agencies?

General LIBUTTI. Sir, as always, you ask the toughest questions and the ones that strike at the heart of what we're all about. And

what we're all about, as I said earlier, is information sharing and infrastructure protection.

The instrumental organization within IAIP that is charged with the backbone, the nerve center, the communications channel for sharing information, is the Operations Center. And then in support of that separate calls, conferences, and meetings attended by General Hughes who runs the IA side, and Bob Liscouski who runs the IP side.

So, let me first say to you, we are very clear on what our mission is. I am very clear what my customer base is, it's the private sector, it's State and local authorities, extending beyond that, but not involved in, the police work. That's the FBI, and the people at the Department of Justice.

But having said that, let me now turn to TTIC, IAIP and what you elude to as being a challenging approach towards dealing with intelligence.

TTIC was established by the Administration and indeed by the President. It was done to integrate intelligence from overseas and foreign sources. It was done to incorporate intelligence and information that is provided by those who focus on intelligence/law enforcement within the domestic scene.

Now, what I am saying to you, or mentioning to you, involves the CIA, the FBI, and by extension the local police forces across the country that have tens of thousands of great cops, who do great things for their community and country everyday.

Now, I am going to try to draw a wiring diagram here, and if I miss the mark, I know that you won't hesitate to pull me back and let me talk in straight and plain English.

You have TTIC here, which is not controlled by CIA, but by the DCI. Now we don't need to, if I may sir, get into an argument about the differences between George Tenet's two hats, but he does indeed wear two hats. And the responsibility that the DCI has is to provide supervisory overview responsibility for TTIC. And indeed, the director at TTIC is a gentleman, who was, or is, in the CIA.

But TTIC is an organization to integrate, fuse, analyze and share domestic and overseas or foreign intelligence. IAIP is both a customer and contributor at TTIC. So is the FBI. So if you say to me, what about this TTIC group, I would say I am part of TTIC and it is sort of like in a religious setting when you talk about the body of Christ and the Catholic Church, that means every Catholic across the face of the globe. We are part of TTIC.

And indeed, on occasion, we challenge and task TTIC who then goes out to its customer base to look at requirements and collection efforts. I'll take a breath and try to move forward, and try to be as organized in my expression as possible.

So TTIC is here. Members of the Department of Homeland Security are part of TTIC. And by extension, that information in a very simplistic diagram, is passed to IAIP. It goes to General Pat Hughes, in the main, and to other members that are part of TTIC. For example, in Customs and Border Patrol, or whatever, it is shared with their parent unit as well. And that is all part of what we're trying to do. There should be an effort to take walls down and not put walls up.

Information comes from TTIC to IA, and IA shares it with IP, because IP can't do the threat assessment risk analysis piece looking at critical infrastructure unless they know what that intelligence picture indicates. IA in the Department of Homeland Security, my operational directorate, looks at sharing information with other members of the customer base; private sector leadership, and State and local authorities.

ORGANIZATION AND STANDUP OF THE TTIC AND ITS FUNCTION

I'm talking there about advisors to the Governors, the homeland security advisors to the Governors. They get that information as well as local authorities. What that means is mayors and their leadership in the intelligence/counter terrorist operations. In most cities across the country, those are the senior police chiefs.

I don't see, Senator Byrd, a conflict in the organization and standup of TTIC and its function. It's function is to integrate. My function and focus is on passing information to my customer base.

I support the FBI who is a partner in this national effort. And they're in the law enforcement business. Fueled by and supported by the same intelligence that's coming out of TTIC. I don't see a conflict. We're improving the way we communicate everyday, we're sharing databases everyday, at a very highly classified level. And we're working more in concert with one another than we ever have.

Leadership in the FBI, the CIA, and the leadership of my organization get it. They understand there needs to be a cultural metamorphosis in terms of information sharing. And we're going to keep working on that so young people in these organizations understand it is one team, one fight, as the Army says. And we need to understand that in terms of information sharing.

I don't see a problem with the current intelligence organization. As always, I work everyday to improve it.

Senator BYRD. Well, General, I understand plain English. But I am not sure that I understand everything that you have said here today. And I am not embarrassed to confess it.

Let me ask a simple question.

General LIBUTTI. Sir.

SECURITY OF THE HOMELAND

Senator BYRD. How is it that our homeland is made more secure by having such a confusing hierarchy of intelligence sharing agencies?

General LIBUTTI. I think that the homeland is much more secure. And I will talk only from my perspective in IAIP, Senator.

We have shared over 70 advisories and alert bulletins in concert with other members of the Homeland Security team. We get threat information from the agency, our friends in the FBI, and, out of TTIC. Then, we look at that, conduct competitive and comparative analysis.

Again, our focus is on our customer base, which includes other members of the Federal Government. So, we take that information, and we pass it on a secure backbone to customers that have clearances. For those who don't have clearances, we take the information that's classified, clean it up, and create what is called the tear line. Then, we coordinate the bulletin or advisory with our friends

in the other intelligence agencies, and we send it out through our Homeland Security Operations Center.

We have sent out many of those advisories. We normally follow up with phone calls to appropriate customers. We call industry leadership to amplify an important point. We send executive teams to places like New York, LA, and Las Vegas, as we did during the holiday period, to share with leadership what we know, and make recommendations on corrective action.

I think, again, as you know, sir, I am sure your staff has briefed you, after 30 years in the Marine Corps and a couple of months at the Department of Defense, I spent a year and a half, as the Commissioner for counter-terrorism in the NYPD. When I finished that job, I came down and was proud to take this job.

If it doesn't work on the streets of our great cities and small towns, it doesn't work for America. And I'm telling you now, sir, we have made a difference.

Senator BYRD. Alright, let us suspend while the reporter changes his tape.

May I ask him another question, Mr. Chairman?

Senator COCHRAN. Yes, sir.

VULNERABILITY ASSESSMENTS AND SECURITY: CHEMICAL INDUSTRY

Senator BYRD. The Department of Homeland Security continues to take a hands-off approach with regard to chemical security by relying on the chemical plant industries. So here we go again, to assess vulnerabilities and take protective actions. We know that the EPA has estimated that if attacked, over 100 plants located all over the country could affect over one million people each.

We know that the Department of Justice released a study in April of 2000, concluding that the risk of terrorists attempting in the foreseeable future to cause an industrial chemical release is both real and credible.

We know that in February 2003, the National Infrastructure Protection Center, which is now a part of the Department of Homeland Security, issued a threat warning that Al-Qaeda operatives also may attempt to launch conventional attacks against the U.S. nuclear, chemical, and industrial infrastructure to cause contamination, disruption, and terror.

When Secretary Ridge testified last year he said that the chemical industry was better suited to assess vulnerabilities and take appropriate security measures than the Federal Government.

Just last week, the General Accounting Office sounded another siren in testimony saying that, in spite of the industry's efforts, the extent of security preparedness at U.S. chemical facilities is unknown.

Do you maintain the position that the chemical industry is better suited than the Federal Government to assess vulnerabilities and take protective actions to secure chemical plants?

General LIBUTTI. It can't be done alone or independently, sir. It is back to the point that I made earlier, it has to be done in partnership. And I think the Federal Government, being gentlemanly in their approach, from time to time, needs to be also muscular. We need to demand standards and guidelines to be adhered to. We

need to be there, prepared to support them in developing their security programs that reinforce their safety programs.

I'm with you 100 percent, sir. I can only tell you that it's a combined effort and everybody needs to pull his or her own weight.

Senator BYRD. Does your budget request address this issue in any way?

General LIBUTTI. Yes, sir, it does.

Senator BYRD. It is so? You said it does. How much is in the budget for this?

General LIBUTTI. In terms of chemical sites security we're talking about \$35 million.

Senator BYRD. And now you're talking about hardening security at chemical plants?

General LIBUTTI. Sir, I'm talking about visits, interaction, working to develop guidelines and the way ahead. We're talking about recommendations for how they can harden their target as we say in the military; standoff distances, excuse me, buffer zones, security plans. We're there to advise, educate, and help them develop their plants. As you know there are tens of thousands of these plants, large and small across the country. And as I said earlier, we looked at and visited over the last few months many of the facilities that we thought were key critical, meaning, if they were hit as centers of gravity, they would cause potentially the greatest impact in the surrounding area.

I am very comfortable that we're taking the right approach on this. And we're going to look at several hundred additional sites or facilities over the next year.

Senator BYRD. What more can you do to make sure that the chemical industry responds with a robust program to secure their plants?

General LIBUTTI. We need to demand excellence across the board. We need to be both their advocate and their coach relative to ensuring that they adhere to standards and best practices. We need to demand excellence in terms of security and should not let them off the hook.

Senator BYRD. You bet. We have lots of work to do in this area.

General LIBUTTI. Yes, sir, we do.

RESEARCH AND TECHNOLOGY INFORMATION DISSEMINATION

Senator BYRD. Now, Mr. Chairman, I shall have further questions perhaps.

Senator Inouye, who could not attend today's hearing, requested that the attached question be asked on his behalf. I ask that it be inserted in the record.

He is concerned that the Department of Homeland Security is charging outside groups that wish to attend a March 8, 2-day forum, that will provide industry with information about homeland security research and technology requirements.

For example, small businesses would be charged \$525, and universities would be charged \$425. Senator Inouye believes this information should be provided free of charge. I ask that his question be made part of the record.

Senator COCHRAN. That objective is so ordered.

Senator BYRD. And I thank both Dr. McQueary and General Libutti.

Dr. MCQUEARY. Thank you, Senator.

General LIBUTTI. Thank you, Senator.

NATIONAL INFRASTRUCTURE SIMULATION AND ANALYSIS CENTER
(NISAC)

Senator COCHRAN. Senator Domenici is attending another meeting of his committee, the Energy Committee which he chairs, this morning. And he asked me to propound a question on his behalf. And it is this:

The fiscal year 2004 Homeland Security Appropriations Act had approximately \$23 million for NISAC. That's the National Infrastructure Simulation and Analysis Center. Would you please give the subcommittee the status of the allocation of the fiscal year 2004 funding? I think that's to General Libutti.

General LIBUTTI. Yes, sir, it is.

I'll try to cut to the chase and cover the key points, sir. As you know this responsibility transferred the Department of Homeland Security from the Department of Energy in March 2003. Primary contractors are the Sandia and Los Alamos labs in New Mexico.

The Senate Appropriations Committee provided approximately \$30 million in 2003, and the House provided \$20 million. Extra dollars from the Senate were dedicated for NISAC building at Kirkland Air Force Base in New Mexico. The joint conference provided \$27.5 million; but there was no specific language for building. But with respect to what the Senator and your colleague had asked for, what we have done most recently, is that we retained sufficient funds to complete the survey and selection process. The date of ground breaking will be dependent upon site surveys and identification of a suitable site for the NISAC.

So we're very attuned to the issue and concern of Senator Inouye. I am happy to provide additional details or perhaps visit with him to provide amplifying information.

Senator COCHRAN. We will submit questions in addition for the record, and if you could respond to those.

General LIBUTTI. I would be happy to, sir.

Senator COCHRAN. For the record, we would appreciate additional detail regarding the fiscal year 2005 budget request for NISAC and activities envisioned in the budget for that Center.

General LIBUTTI. I would add, sir, that our department is preparing a letter to the Department of Defense regarding building of a facility on the Department of Defense property, et cetera, et cetera. So, we'll be happy to provide response and detail.

Senator COCHRAN. Thank you.

MANPADS/AIR MISSILE COUNTERMEASURES

Following up on another issue that was raised by Senator Byrd. Is it feasible to accelerate the shoulder-fired missile defense program to make the technology available at an earlier date? Or, is the time line you have considered the most cost effective, or reasonable in terms of the needs for a cost efficient method of protecting commercial aviation?

Dr. MCQUEARY. We believe that the time line is a very aggressive time line, and in fact, we're certainly aware that there is great interest in the country about the very issue that you raised. When we met with each of the three contract winners, posed to them the following question: Would you like to come in and recommend a shorter schedule. None of the three agreed that they would be willing to take on, or would want to take on, a schedule that was shorter than the one that we had originally proposed.

So, I think it is an aggressive schedule, and I think a careful examination of what we have to do in the allotted time period would conclude that is the case.

Senator COCHRAN. Has there been any decision made or discussion of who's actually going to pay the costs of procuring and outfitting the airliners with this defense system? I understand that they estimated costs could be up to \$10 billion.

Dr. MCQUEARY. There are a number of factors that go into that. We have not attempted to address, however, who would pay for it. We have attempted to address how much it would cost, though. So those decisions can be made. As I indicated earlier in the testimony, we view our responsibility as providing the scientific basis on which the Administration and the Congress can decide the approach the country will take in implementing such systems, if that is what we should do.

We put target costs in of about \$1 million each, but that's up front hardware costs. And anytime you field large systems, operation and maintenance typically dominates the overall long term costs of such systems. And I would expect that is the case on this one.

CYBER SECURITY

Senator COCHRAN. We know that you have recently developed a national cyber alert system to acquaint home computer users, and business and government agencies, with ways to better secure their computer systems from viruses. How would you rate the performance of the new national cyber alert system's response to the most recent computer virus outbreaks?

Dr. MCQUEARY. That was done by General Libutti's organization. I'll defer to him if I may.

Senator COCHRAN. Sure.

General LIBUTTI. Sir, I would give you an estimate on a scale of 1 to 10, at 8.5 or 9. And that's a relative evaluation. Let me give you some additional information that perhaps would help understand where we are. This roll out of the alert system has just been done very recently.

We have over 250,000 subscribers. Those who have subscribed to that system, are working that system across industry, home users and government. We think, I believe, it is the first great move to educate, inform and make people aware in a pro-active way, of viruses that may be coming our way.

So I give it a pretty high grade, and we will continue to monitor that as time goes by, and improve on how we communicate with our customer base.

Senator COCHRAN. What's the relationship between the cyber security division and TTIC; if any? Is there any collaboration?

General LIBUTTI. I mean in terms of a wiring diagram, if I may, there is no direct linkage. There is always within the Federal Government, particularly the inter-agency, there's linkages and pathways that permit people who work in the cyber business to communicate with people who have that interest, or that particular functional area of responsibility within TTIC.

That is, there are people in TTIC who not only look at infrastructure protection from a threat perspective, but also can consider cyber concerns. The key point that I leave with you is, that the lead in terms of cyber security is within IAIP at the Department of Homeland Security.

If we have issues that present themselves, then we will orchestrate appropriate meetings. There was an initiative taken by some of my folks in the cyber world to take a hard look at what I call a lower level inter-agency grouping between the communication folks, the national communication security guys, or guys in cyber security, and the Department of Defense. They met on a regular basis to review potential threats, and to look globally at the kind of activity that needs, to in my words, give us a warning and indicator that we need to do something.

So we're trying to be as pro-active as possible, and we're trying to educate and make people aware of the threat to the cyberspace area.

CYBER SECURITY

Senator COCHRAN. How is the national cyber security division working with the private sector companies, such as Symantec, McAfee, and Norton, that specialize in anti-virus software and internet security.

General LIBUTTI. I think it's safe to say they're working very well with them. Briefings I have received have indicated no serious problems in terms of our linkage and cooperation with the business community overall.

ADDITIONAL COMMITTEE QUESTIONS

Senator COCHRAN. What law enforcement agency has primary jurisdiction in enforcing cyber crimes?

General LIBUTTI. I suspect again across law enforcement, and that's not my area of expertise, that it is both Secret Service and FBI.

[The following questions were not asked at the hearing, but were submitted to the Department for response subsequent to the hearing:]

QUESTIONS SUBMITTED TO THE SCIENCE AND TECHNOLOGY DIRECTORATE

QUESTIONS SUBMITTED BY SENATOR THAD COCHRAN

BIOSURVEILLANCE SYSTEM

Question. Science and Technology's role in the Biosurveillance Initiative includes an increase of \$65 million to expand environmental monitoring activities in cities determined to be at the highest risk of a terrorist attack.

Can you give further details about the chemical and biological warning activities currently in place in these cities?

Answer. The U.S. Department of Homeland Security's (DHS) BioWatch initiative has been successfully operating in approximately 30 of the Nation's urban centers

since early 2003. BioWatch is an early warning system that can rapidly detect trace amounts of biological materials in the air whether they are due to intentional release or due to minute quantities that may occur naturally in the environment. Routine air samples are collected on a daily basis and more frequently if necessary. To date, BioWatch has analyzed well over half a million samples. Several hundred specialized air sampling devices, developed by the Department, have been placed at key locations nationwide. The air samplers are supported by the infrastructure set up by the Environmental Protection Agency's (EPA's) Air Quality Monitoring Network sites in partnership with State, local and tribal environmental agencies. Additional partners in the program include the Centers for Disease Control and Prevention (CDC) and the Department of Energy (DOE) National Laboratories. The CDC provides technical expertise through its Laboratory Response Network on the laboratory analysis methods and serves as the liaison for laboratory analyses with State health departments. The DOE National Laboratories, specifically Los Alamos and Lawrence Livermore National Laboratories, provide technical expertise in biological sampling systems, laboratory analysis, and training assistance to State and local agencies.

Question. If the requested increase in funding is provided, will the monitoring be expanded to other cities that are currently being monitored or just in these high-threat areas? What about other high-threat areas designated under the Office for Domestic Preparedness grant programs?

Answer. The current planning calls for significantly increasing the number of air samplers in the top ten high-threat BioWatch cities only. Given availability of funds some modest addition of other cities may be possible in the future.

The Science and Technology (S&T) Directorate coordinates with the Office for Domestic Preparedness (ODP) to insure integration of BioWatch capability with cities listed on the Urban Area Security Initiative (UASI). The DHS S&T BioWatch Program fully funds the installation, operation, and sustainment of the BioWatch system in each city. The ODP grants program is complimentary to BioWatch and funds first responder initiatives and other local high priority requirements.

Question. What promising new advances do you anticipate with the requested increase in funding for the acceleration of research and development on next generation environmental monitoring systems?

Answer. Accelerated research and development on next generation detection systems fall into two categories: (1) outdoor wide area environmental monitoring (i.e., BioWatch replacement) and (2) indoor facility protection. Research and Development (R&D) programs for the wide area environmental monitoring focus on autonomous networked detectors. This is a self-contained on-site collection and analysis system. To address indoor facility protection the R&D plan calls for research to develop Rapid Identifiers—portable highly sensitive bioagent detectors with very low false alarm rates.

COUNTER MAN PORTABLE AIR DEFENSE SYSTEMS (MANPADS)

Question. The Science and Technology Directorate is currently in the early stages of a 2-year, \$120 million program to develop countermeasures to protect against the threat of shoulder-fired missiles on civilian commercial aviation.

What progress is being made by the three teams selected for the Counter-MANPAD Program, and is the first phase on schedule to be completed this summer?

Answer. In early October, 2003, the Department of Homeland Security's Science and Technology Directorate released a solicitation announcing a "call for proposals" to address this potential threat. The solicitation is the first step in the Department's two-phase systems development and demonstration program for anti-missile devices for commercial aircraft.

Phase I began in January, 2004, with the selection of three contractors—BAE Systems, Northrop Grumman, and United Airlines. Phase I of the program will provide a detailed design and an analysis of the economic, manufacturing, operational, and maintenance issues needed to support a system that will be effective in the commercial aviation environment. This phase will last approximately 6 months and will end in the selection of one or two contractors moving on to the next phase.

The Counter-MANPADS program is on track. The DHS Special Project Office (SPO) conducted meetings with all three contractors in late January, 2004, and early February, 2004, to establish firm direction and expectations. The SPO completed System Requirements Reviews with all three contractors by March 18, 2004. An Interim Design Review will be conducted in early May, 2004. These reviews establish a firm baseline of requirements against which the contractors can apply their designs.

Phase I will conclude with a Preliminary Design Review in July, 2004, at which time the DHS will select one or two of the initial three contractors to proceed into Phase II.

Phase II will include development of prototypes, integration onto commercial aircraft, and demonstrations of system operation and performance. These prototypes will also be subjected to a rigorous test and evaluation process. Phase II will last approximately 12–18 months followed by a recommendation to the Administration and Congress.

Question. What obstacles do you face in safely applying technologies developed for and currently in use on military aircraft and adapting a countermeasure system to operate in the environments of civilian aircraft?

Answer. Technologies developed for military or other specialized purposes are currently incompatible with commercial air fleet operations. Although underlying military technologies will be leveraged, the systems must be adapted to meet commercial operational conditions and environments.

Military missile countermeasures exist in various stages of development and initial fielding. However, these technologies are generally utilized by military and Heads-of-State aircraft that have the operations and maintenance infrastructure to support such systems.

While it is conceivable that existing military countermeasures units could be re-engineered for civilian aircraft use, many technical and operational tradeoffs have not been previously performed to address risks of such approach. For example, there is an established military logistics infrastructure that serves airborne countermeasure equipment, spanning functions from pilot training and routine maintenance to spare parts and depot repair. A similar infrastructure would be costly and time-consuming to replicate in the commercial airline industry.

It would be premature to integrate currently available military countermeasures equipment aboard civilian aircraft due to numerous issues concerning aircraft modification and certification, maintenance and supportability, and operational employment. The current Counter-MANPADS Program aims to resolve such issues and to provide alternatives to the Administration for a decision on equipping commercial aircraft with Counter-MANPADS capabilities.

Additional details can be provided if desired in accordance with the appropriate security for the information.

Question. Is it feasible to accelerate the Counter-MANPAD Program in order to make the technology available at an earlier date, or is the timeline proposed the safest and most cost-efficient method?

Answer. Given the challenges of migrating Department of Defense (DOD) technology into the commercial aviation environment, the DHS program is the most cost-efficient approach to implementing an affordable system. The program is an aggressive 24-month analysis, prototype demonstration and testing program. At the conclusion, the Department of Homeland Security will provide the Administration and Congress with a recommendation for the most viable solution to integrate Counter-MANPADS technology into commercial air fleet operations.

CYBER SECURITY

Question. The Science and Technology Directorate serves a role in the Nation's cyber security efforts by addressing cyber threat characterization, cyber threat detection, and cyber threat origination.

With the large increase provided to the Science and Technology Directorate by Congress for cyber security research and development, what advances can we expect during this fiscal year?

Answer. The funding increase provided by Congress is enabling the Science and Technology (S&T) Directorate to undertake cyber security programs that would not have been possible otherwise. As fiscal year 2004 is the first complete fiscal year of the Department of Homeland Security's existence, funding investments this fiscal year emphasize infrastructure and foundational needs associated with cyber security. Because such needs are generally not associated with short-term problems, most of these investments will not result in deployable advances in the same year in which efforts are undertaken. However, several key areas are being addressed and are briefly described in the following text.

In order to address infrastructure needs identified in the National Strategy to Secure Cyberspace, the Cyber Security R&D Portfolio in the S&T Directorate has initiated activities aimed at securing some of the key basic communication protocols on which the Internet relies, but which are presently vulnerable to cyber attacks. A program focused on the domain name infrastructure is working to advance the diffusion and use of the Secure Domain Name System (DNSSEC) protocol as a replace-

ment for the traditional domain name infrastructure. A second program aimed at secure routing infrastructure is working to address vulnerabilities in Border Gateway Protocol (BGP), the protocol associated with the Internet's underlying routing infrastructure.

A second infrastructure need identified in the National Strategy to Secure Cyberspace involves the need for improving the security of process control systems, such as supervisory control and data acquisition (SCADA) systems and digital control systems (DCS). The Cyber Security Portfolio is coordinating planning for these areas with the Critical Infrastructure Protection Portfolio. These portfolios expect to initiate joint activities in this area later this fiscal year.

The S&T Directorate is also working to provide foundations for enhancing the capability of a variety of cyber security research communities. The Cyber Security R&D Portfolio is co-funding two multi-university test bed projects with the National Science Foundation (NSF). The first is a test bed project focused on creating a large-scale physical test bed network to support testing activities, and the second test bed project focused on developing a testing framework and conducting experiments on the physical test bed. These activities will result in the ability to conduct attacks, develop an understanding of those attacks, and test existing and new technological cyber security concepts, all in a large-scale operational network environment that is kept isolated from the "public" Internet.

A separate effort aimed at supporting cyber security research and development communities is a program that is working to develop large-scale data sets for cyber security testing. This will address the need that researchers and operational users have for realistic data that can be used to test the capabilities of current and emerging cyber security technologies. Although the S&T Directorate does not expect to play a role in the area of testing, evaluating, or certifying commercial technologies, the general approach to constructing and making available data sets for testing have the potential for secondary benefits by catalyzing the emergence of commercial testing services provided by and for the private sector.

Another area of emphasis is the area of economic assessment. This activity is focused on two important priorities. The first is developing a general model for assessing the economic impact of cyber events and attacks. We do not believe that widely touted figures (such as \$38 billion for a single Internet worm attack) are realistic estimates of cost associated with those attacks. Unrealistic figures do the private sector a disservice because they do not allow people to make reasonable assessments of their security needs and associated investment requirements. The second area of interest is the development of tailored business cases aimed at different types of stakeholder communities. General awareness campaigns aimed at widespread improvements in cyber security have not been as successful as one would like. We believe that one of the reasons for this is that the rationale for supporting cyber security investments needs to be tailored to different types of stakeholder perspectives (large enterprises, critical infrastructure sector company, small businesses, home users, etc.). It is our hope that such tailored business cases will provide better rationale for technology investments both among today's commercial cyber security technologies, as well as those of the future.

The activities described above fit into a coherent plan for long term cyber security needs. It is our hope that the test bed/testing framework projects and the program focused on large-scale data sets will provide insights to support the development of cyber security metrics, although additional work in this area is expected to emerge from NSF-funded basic research programs. In the long term, the general areas of cyber security metrics and economic assessment models will provide two key components in developing a foundation for cyber security risk assessment, and risk-based decision-making in this field.

Although the emphasis of fiscal year 2004 activities is on infrastructure and foundational needs, this is not to the exclusion of other activities. We do have plans for a number of other focused activities, including conducting a pilot test of new-generation intrusion detection technology with participation from the banking and finance sector, and holding a workshop in the area of government needs for wireless security to gather input for future R&D activities. In fiscal year 2005, with the infrastructure and foundational programs already in motion, we expect to expand our activities aimed at more specific cyber security technology R&D needs.

Question. How will the Science and Technology Directorate coordinate its activities with the Information Analysis and Infrastructure Protection Directorate?

Answer. The Director of Cyber Security R&D in the S&T Directorate is working closely with counterparts in the Information Analysis and Infrastructure Protection (IAIP) Directorate to coordinate the Directorates' relevant activities in the important area of cyber security. The two components of IAIP that S&T has been working with are the National Cyber Security Division (working with the Director of the Division

and other senior staff members) and the National Communications System (working with the Chief of the Technology and Programs Division and other senior staff members).

Interactions between the two Directorates include an ongoing series of meetings between senior-level technical managers to provide a bi-directional flow of information between the organizations as well as coordination of technical activities. These meetings are aimed at ensuring that DHS operational requirements feed into S&T programs, and to help identify paths for diffusion of technology back out to end users, as outcomes of these programs begin to emerge. On a more ad hoc basis, the S&T and IAIP Directorates exchange invitations to attend meetings or workshops when they involve areas of common interest.

The IAIP Directorate has been developing a written document to identify its S&T requirements, and expects to provide this document to the S&T Directorate upon its finalization. In the longer term, a Science and Technology Requirements Council (SRC) is being established within DHS to provide a more formal avenue for IAIP and other DHS components to communicate requirements to the S&T Directorate across all of the technology portfolios.

Question. Have other agencies within the Department of Homeland Security, such as the Secret Service, the Coast Guard, and the Transportation Security Administration, begun to outline their cyber security requirements?

Answer. The Director of Cyber Security R&D has been informed of several information technology-related requirements related to the Secret Service's mission via IAIP and via the Secret Service Portfolio Manager in the S&T Directorate. While related to information technology, several of these requirements have been identified as having a law enforcement component being outside of the scope of cyber security.

The S&T Directorate has not been approached by the Coast Guard or the Transportation Security Administration (TSA) regarding their cyber security requirements. We have had discussions with the Federal Aviation Administration regarding their cyber security R&D priorities, which are focused on securing the aviation infrastructure (e.g., air traffic control networks), in contrast to TSA's focus on passenger and cargo security.

HOMELAND SECURITY CENTERS OF EXCELLENCE

Question. The Nation's universities have begun to join the Department of Homeland Security to combat terrorism with the selection in December of the first Homeland Security Center of Excellence which will focus on the risk analysis related to the economic consequences of terrorist threats and events. The process of selecting the next two Homeland Security Centers of Excellence to focus on agro-terrorism is currently in progress.

How many additional Homeland Security Centers of Excellence do you envision with the \$69 million provided for fiscal year 2004 and with the \$30 million requested in the President's budget to accompany the three mentioned?

Answer. Fiscal year 2004 funding for University Programs will include approximately \$10 million for the DHS Scholars and Fellows Program, with the balance dedicated to University-based Homeland Security (HS) Centers. In addition to the risk analysis and agro-terrorism centers referenced in your question, we anticipate two more solicitations for University-based Homeland Security Centers this fiscal year.

Question. How will the Science and Technology Directorate coordinate the Homeland Security Centers of Excellence research and findings among each participating university?

Answer. Lead universities are required to develop a management plan that demonstrates that partners will be communicating and reporting results and findings on a regular basis. DHS requires regular written reports and assigns a program manager to each HS Center of Excellence. Additionally, lead universities are required to form Science Advisory Panels, to conduct progress meetings with their partners, and to participate in review meetings with DHS senior managers. As new HS Centers are added, DHS envisions a system of centers that it will coordinate. Findings from these centers will be coordinated and consolidated by DHS.

BIOLOGICAL COUNTERMEASURES

Question. In addition to the national biosurveillance initiative proposed in the President's budget in the biological countermeasures portfolio, additional funding is requested for infrastructure improvements at the Plum Island Animal Disease Center.

How is the Department of Homeland Security currently working with the United States Department of Agriculture to coordinate research being carried out in regard to biological diseases?

What countermeasures are being prioritized for agro-bioterrorism?

As this committee makes recommendations to fund infrastructure improvements at the Department's research facilities, what intentions do you see for the long-term use of Plum Island as part of Science and Technology's National BioDefense Analysis and Countermeasures Center?

Answer. DHS is totally committed to enhancing the Nation's agricultural security by complementing the mission of United States Department of Agriculture (USDA) and Food and Drug Administration (FDA), and bringing a new sense for urgency and investments to enhance the Nation's capability to anticipate, prevent, detect, respond to, and recover from the intentional introduction of foreign animal disease, especially scenarios of high-consequence. As defined in Homeland Security Presidential Directive-7 (HSPD-7) and HSPD-9, the Secretary of Homeland Security is responsible for coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States, including the defense of agriculture and food.

Agriculture and food security are important priorities for DHS, as are its working relationships and interactions with key sector-specific agencies. DHS utilizes high-consequence reference scenarios for strategic planning for its programs and activities on biological and chemical countermeasures and these areas are most relevant to protecting the agriculture and food sectors. DHS works closely with the respective sector-specific agencies in planning and execution of its R&D programs for each scenario. Of seven scenarios currently under study, two of the four biological scenarios concern agriculture and food security: foreign animal disease (with an initial focus on foot-and-mouth disease), and bulk food contamination. We will be working extensively with the USDA on response to those scenarios.

A Joint DHS and USDA Working Group on Agricultural Biosecurity has developed a partnership and national strategy to provide the best possible protection against the intentional or accidental introduction of a foreign animal disease. The strategy builds on the strengths of each agency to develop comprehensive preparedness and response capabilities.

USDA's Agricultural Research Service (ARS) has traditionally excelled in basic and fundamental science and early disease discovery research. USDA's Animal and Plant Health Inspection Service (APHIS) has provided diagnostic services for a wide range of foreign animal diseases. In the partnership strategy, USDA will continue its basic and early discovery work in the areas of foot-and-mouth disease and other high priority foreign and emerging diseases, diagnostic development, and maintenance of the vaccine bank.

DHS's program at Plum Island Animal Disease Center will focus on strengthening the Nation's ability to predict and respond to the intentional introduction of a foreign animal disease into U.S. agriculture. DHS is focusing its efforts on:

- Advanced development which evaluates the efficacy of vaccines and therapeutics (antivirals) derived from ARS's discovery work and moves them into readiness for application in the event of an outbreak;
- Agricultural agent bioforensic analysis capability to support attribution, working in conjunction with APHIS's diagnostic laboratory and law enforcement agencies;
- Disease assessment capability to include risk, threat assessment, and epidemiologic resources to augment knowledge about specific strains of foreign animal diseases for use in decision making and predictive disease modeling; and
- Supporting the functions of the core scientific units such as pathology, microscopy, sequencing, animal studies, strain repositories, and bioinformatics.

The combined programs of DHS and USDA at Plum Island Animal Disease Center will enhance the Nation's defense by building on the strengths of each agency to increase capacities for both research and diagnostic technology development.

As part of DHS's extensive commitment to agricultural security, it is also establishing two University Homeland Security Centers in this area: one in foreign animal and zoonotic diseases and one in post-harvest food security. These new HS Centers were awarded to Texas A&M University and the University of Minnesota respectively. Additionally, DHS is coordinating with USDA on a review team for high-consequence reference scenarios for strategic planning for DHS's programs and activities on biological and chemical countermeasures. DHS is also conducting end-to-end system studies to help define the requirements for detection and surveillance for agricultural outbreaks and for the protection of critical nodes of high consequence in the food production chain.

DEPARTMENT-WIDE RESEARCH AND DEVELOPMENT

Question. Currently, Science and Technology provides mission support for several agencies within the Department of Homeland Security to coordinate research and development throughout the Department to prevent redundancies and to provide overall management and oversight of ongoing research. The President's fiscal year 2005 budget proposes further consolidation of research and development within Science and Technology.

How do you feel the consolidation of research and development of nearly all agencies in the Department of Homeland Security into Science and Technology will provide for better coordination of research and more efficient use of the funds provided?

Answer. Consolidation of the research and development functions of the Department's components will significantly improve the Department's overall ability to meet its mission. With consolidation, we can ensure that operational end-user requirements and needs are being met by the best science and technology that can be brought to bear on the problem, whether that expertise comes from internal or external sources. We will enhance our ability to avoid duplication of effort in the R&D areas, and we fully expect to find synergies develop: what is created to meet the requirements of one component may be able to be fielded to support the needs—stated or not yet recognized—of another.

Question. What examples can be given of different agencies benefiting from another agency's research that can be attributed to the centralization of these efforts?

Answer. The Department's consolidation process has truly just begun. Our experience to date has been in supporting other components of DHS at the portfolio level. We have staff in the S&T Directorate who are liaisons with other DHS components; specifically the Border and Transportation Security Directorate, the United States Coast Guard, the Emergency Preparedness and Response Directorate, the United States Secret Service, and the Information Analysis and Infrastructure Protection Directorate. These liaisons bring forward the requirements from these other components, which allows us to factor their needs into the S&T Directorate's RDT&E planning and budgeting and they also serve as a communication link at the portfolio level.

The consolidation of the Standards efforts earlier in DHS has already resulted in a more effective and efficient process to identify and implement standards relevant to the entire DHS mission. The results to date include:

- 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.

Question. How does the Transportation Security Administration's laboratory coordinate its efforts with Science and Technology, and, more specifically, the High Explosives Countermeasures portfolio, and do you anticipate the consolidation of the Transportation Security Administration's research and development into Science and Technology?

Answer. For fiscal year 2004 the S&T Explosives Countermeasures Portfolio has initiated research, development, testing and evaluation (RDT&E) to counter the explosives threat to the general population and to critical infrastructure posed by suicide bombers and vehicle bombs, respectively. The Transportation Security Administration (TSA) is conducting RDT&E to counter the explosives threat to the transportation sector, including land and maritime transport as well as civil aviation. S&T and TSA keep each other aware of activities being performed; thus, redundancy is minimized. The activities are currently not coordinated, however, and priorities are set independently. Information exchange between the S&T Explosives Portfolio and the TSA laboratory is coordinated through the TSA office of the Chief Technology

Office. Each group calls upon the expertise of the other when warranted, including participation in selected project reviews and advisory panels. It is anticipated that the RDT&E activities currently conducted within TSA will be consolidated within Science and Technology commencing in fiscal year 2005 following administrative actions and agreements that are in progress. Program planning documents for the Explosives Countermeasures Portfolio reflect an integration of current S&T and TSA mission areas, priorities, and funding profiles.

Question. How does Science and Technology prioritize research across all Departmental agencies?

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

- Homeland Security Act of 2002;
- The fiscal year 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. As consolidation continues to occur, these same sources will be used to prioritize requirements and needs.

We will continue to improve our ability to garner customer requirements through the newly-formed Science and Technology Requirements Council (SRC). The SRC will vet RDT&E requirements from the other components of the Department and has Assistant Secretary level representation from those components.

INTERAGENCY COORDINATION OF HOMELAND SECURITY RESEARCH EFFORTS

Question. What type of coordination is occurring with other Departments in their research and development efforts, and how do you plan to expand this coordination in the future?

Answer. The Department of Homeland Security fully recognizes that many organizations contribute 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 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.

We are now working to identify gaps in homeland security programs across all relevant Federal Departments and agencies. We are participating in—and in some cases, leading—committees, subcommittees, and working groups of the National Science and Technology Council (NSTC). Through formal and informal conversations at NSTC meetings, gaps are being identified and are starting to be addressed.

In addition, staff from the S&T Directorate are actively involved with the Counterproliferation Technology Coordinating Committee (CTCC). The CTCC's role is to look across the U.S. Government to identify counterproliferation activities, iden-

tify gaps and shortfalls, and make recommendations to address the shortfalls. Many of the technologies relevant to Counterproliferation also are relevant to Homeland Security needs. The CTCC is co-chaired by the National Security Council, Homeland Security Council and Office of Science and Technology Policy.

The Office of Management and Budget (OMB) gives us budgetary direction and develops a yearly report on Combating Terrorism. This document is one of the sources cited above as guidance for program prioritization. We have frequent interactions with OMB for guidance in budgeting in accordance with identified priorities.

Question. The Office of Science and Technology Policy (OSTP) is one of our most important connections in the Administration. Our personnel meet with OSTP staff frequently on issues of interest to both groups. Most importantly, OSTP runs the National Science and Technology Council and its committees, subcommittees and working groups as mentioned above. These groups are instrumental in helping us achieve our goals of protecting the Nation and its infrastructure.

The Homeland Security Council, (HSC) which was stood up in October 2001, meets frequently to ensure coordination of all homeland security-related activities among executive departments and agencies and promote the effective development and implementation of all homeland security policies.

Has there been any thought given to creating a multi-agency initiative, or working group, perhaps under the auspices of the National Science and Technology Council (NSTC), to foster better coordination of Homeland Security Research efforts across government agencies (e.g. DOD, NIH, NSF, DOE, Transportation, EPA, USDA, Dept. of Justice, etc)?

Answer. As discussed above, the Science and Technology Directorate is working with the NSTC and the CTCC to look across the entire Federal Government at homeland security-relevant science and technology.

RAPID PROTOTYPING

Question. The Congress made \$75 million available for fiscal year 2004 for the rapid prototyping and deployment of near-term technologies for the end-user, whether it is a Customs agent or a first responder, to have the best technology and equipment available to combat terrorism.

How do you propose to better streamline the process of working with industry to make technology available to the end-user in a more expeditious manner than currently available?

Answer. The Science and Technology Directorate actively promotes a close relationship with industry to produce the new, improved technologies that emergency responders will purchase. Since March 1, 2003, there have been four solicitations directly to industry in 63 high tech areas related to protection, equipment, sensors, and other gear for emergency responders, agents, detection and tracking systems. Industry sent in more than 4,500 responses to these solicitations. Our partner, the Interagency Technology Support Working Group (TSWG) is awarding \$60 millions in contracts now in these areas. Our Office of Systems Engineering and Development (SED) is already at work with three industry teams on technology for commercial aircraft to counter shoulder-fired missiles. The Homeland Security Advanced Research Projects Agency (HSARPA) has been able to shorten the time required for a complete, multimillion dollar competitive solicitation to just 120 days. HSARPA is also using "industry-friendly" Other Transactions for Research and Prototype contracting authority permitted by the authorizing legislation to speed award of contracts to companies that have not done business with the government before.

Question. Of the industry response to the Department's request for proposals, what technologies have proved to be the most beneficial to homeland security?

Answer. DHS S&T is in the earliest stages of research and development for almost all of these efforts and it would be premature to judge which of these technologies will be most beneficial.

Question. What future technology solicitations do you anticipate to better serve the end-user in protecting the homeland?

Answer. DHS S&T is actively pursuing additional technology solicitations in several areas relevant to protecting the homeland. Currently HSARPA has a solicitation entitled "Detection Systems for Radiological and Nuclear Countermeasures" which is now active and industry is responding. Eight other solicitations planned for this year:

- Bioinformatics and Assay Development Program
- Threat Vulnerability, Testing, and Assessment
- Automated Scene Understanding
- Advanced Container Security Device
- Bomb Interdiction for Truck and Suicide Threats

- Biological Warfare Architectures Study (Food & Agriculture)
- Biological Warfare Decontamination
- Low Vapor Pressure Chemical Detection System

Question. Of the funds provided for and the flexibility given to Science and Technology for rapid prototyping, how much is provided for the Technology Clearinghouse, and how much is provided for the Technical Support Working Group?

Answer. For fiscal year 2004, the Technology Clearing House will receive \$10.5 million. For fiscal year 2004, DHS S&T provided \$30.0 million to the Technology Support Working Group (TSWG) for Rapid Prototyping projects.

STANDARDS

Question. Congress transferred the development of standards from the Office for Domestic Preparedness (ODP) to Science and Technology and therefore expects all standards development in the Department to be centralized in the Science and Technology Directorate.

How is Science and Technology coordinating with the National Institute of Standards and Technology (NIST) in developing standards Department-wide?

Answer. The standards development work in ODP was managed by the NIST Office of Law Enforcement Standards (OLES). There has been a smooth transition of this program in fiscal year 2004 as NIST/OLES is still managing the program for the Science and Technology Directorate. The S&T Directorate is also working with NIST to coordinate development of additional standards in other areas, such as biometrics, cyber security and detection methods for weapons of mass destruction (WMD).

Question. How are the State Homeland Security Advisors providing input for the end-users in developing standards?

Answer. The DHS Office of State and Local will provide points of contact for specific standards development efforts. Also, the Conference of Radiation Control Program Directors (CRCPD) has been involved in user requirements for the first set of radiation detector standards.

Question. Do you anticipate Science and Technology will publish a “Consumers Report” on all technologies and equipment for Federal, State, and local users, such as the report that will be published for radiation and bioagent detection devices?

Answer. It is our intention to publish user guides to available technologies in something like a “Consumers Report” format for critical equipment for emergency responders. These guides will address personal protective equipment as well as detectors for chemical, biological, radiological/nuclear and high explosive agents.

THE WIRELESS PUBLIC SAFETY INTEROPERABILITY COMMUNICATIONS (SAFECOM) PROGRAM

Question. The problem of communications interoperability for first responders, so important since September 11th, remains a difficult nut to crack. How much will be needed to fund the solution? When will technical standards be completed? What should the States and locals do? The Science and Technology Directorate plays a lead role for the Federal Government for finding the way through all of the technical questions. The Wireless Public Safety Interoperability Communications Program—known as SAFECOM—is in the Science and Technology Directorate. Yet, no funds are directly requested in the Science and Technology Directorate budget for this very important program. All of the funding comes either from other Federal agencies or from the Department-wide Technology appropriations within the Department of Homeland Security.

Answer. There is no simple solution for communications interoperability. To ensure that our emergency responders’ wireless communications are fully interoperable will require years of hard work on the part of the Federal Government as well as cooperation from State and local entities. The Wireless Public Safety Interoperability Communications Program, SAFECOM, is managed by the Department of Homeland Security’s Science and Technology Directorate, allowing the program full access to the scientific expertise and resources needed to help our Nation achieve true public safety wireless communications interoperability.

Current estimates of total funding required for complete interoperable wireless communications run into the billions of dollars when procurement grants are included in these estimates. Full wireless communications interoperability is currently estimated to be complete by 2023.

Technical standards are critical to the development of interoperable systems. With input from the user community, portions of the Association of Public Safety Communications Officers (APCO) Project 25’s existing, but still incomplete, suite of stand-

ards have been developed. However, adoption has been slow, and standards completed to date address only part of the problem.

SAFECOM will dedicate funding to the implementation of its standards plan, calling for a common set of standards, policies, and procedures to drive the migration of systems towards advanced, interoperable equipment and processes in the future. SAFECOM recognizes that the Nation cannot wait for a complete suite of standards. In the interim, local and State agencies must make investments that improve their communications and interoperability capabilities. To support the practitioner community in the short term, SAFECOM will begin a number of initiatives to better inform public safety agencies when upgrading or replacing current communications systems.

Question. Should the funding for SAFECOM within the Department of Homeland Security be appropriated directly to the Science and Technology Directorate?

Should funding be provided by Science and Technology for research being carried out for SAFECOM?

Should the funding provided by other agencies be permanently transferred to the Department of Homeland Security?

Answer. In an effort to coordinate the various Federal initiatives, SAFECOM was established by the Office of Management and Budget (OMB) and approved by the President's Management Council (PMC) as a high priority electronic government (E-Gov) initiative. As an e-Gov initiative, it is appropriate for funding to be provided by the partnering agencies that will benefit from the results of the initiative.

Question. The progress being made on setting the technical standards for various communications technologies seems to be progressing very slowly. Project MESA which will govern broadband technology is in its infancy, and Project 25 governing Land Mobile Radios has yet to complete even half of the standards necessary. What more can be done to ensure the speedy completion of these projects by the private industry and public safety community stakeholders?

Answer. At a strategic planning session in December 2003, public safety stakeholders from the local, State, and Federal levels convened to determine the most important next steps for the improvement of public safety communications and interoperability. These stakeholders felt that a process to promote standards is critical. To meet this demand, SAFECOM has developed a plan to accelerate the development of critical standards for public safety communications and interoperability, including the Project 25 suite of standards (P25). As mentioned above, SAFECOM will dedicate funding to the implementation of its standards plan, calling for a common set of standards, policies, and procedures to drive the migration of systems towards advanced, interoperable equipment and processes in the future. In addition, SAFECOM will fund the testing and evaluation of interim technologies that can assist public safety agencies in making existing legacy equipment interoperable with other neighboring systems.

QUESTIONS SUBMITTED BY SENATOR TED STEVENS

Question. What types of research and development support will the Science and Technology Directorate provide to the Coast Guard for its non-homeland security missions?

Answer. The Science and Technology Directorate and United States Coast Guard (USCG) are in the midst of preparing a formal agreement that will detail the coordination and funding mechanisms for USCG R&D capabilities. The foundation for that agreement will be the consolidation of funding requested in the fiscal year 2005 budget. For fiscal year 2005, the USCG R&D center facility, personnel and maintenance expenses will be funded through S&T in the amount of \$13.5 million. In addition, S&T and the USCG have agreed upon a base level of additional project funding in the amount of \$5 million that will be specifically targeted toward non-security related projects including maritime science and research. This funding will be designed to support USCG mission-programs such as Marine Environmental Protection, Living Marine Resources, Search and Rescue, Aids to Navigation and Marine Safety. The specific projects in support of these mission-related programs will be prepared annually for S&T concurrence.

In addition, the USCG will submit security-related research requests through S&T for coordination across all portfolios and DHS components. The Coast Guard has submitted a maritime security R&D portfolio detailing approximately \$50 million in vital maritime security research initiatives. This portfolio has been validated by S&T portfolio managers and will be considered in the development of future spending priorities and commitments from S&T.

Question. Will the Department of Homeland Security develop a Homeland Security Center dedicated to energy production security and pipeline infrastructure protection?

Answer. The Department of Energy (DOE) is designated as the lead agency for security issues specific to the energy sector (except for commercial nuclear power plants, for which DHS and the Nuclear Regulatory Commission are designated as responsible lead agencies) in the National Strategy for Physical Protection of the Critical Infrastructure and Key Assets and in Homeland Security Presidential Directive-7 (HSPD-7).

DHS has the lead for transportation systems security which includes pipelines. DHS has overall homeland security responsibility and recognizes that the energy sector is especially vital to the quality of life and the economy of this Nation. DHS is sponsoring Critical Infrastructure Protection research and development programs in the energy and pipeline security area with emphasis on Supervisory Control and Data Acquisition (SCADA) and electronic control systems. These efforts will increase this fiscal year. In addition, DHS asked the National Academy of Science to host a workshop to provide DHS with advice and guidance on future University-based Homeland Security R&D Centers. The results of that workshop did not place energy production security and pipeline security infrastructure in the top three areas recommended as additional areas for potential University-based Homeland Security Centers. This result certainly does not imply these infrastructures and their security is are not important, and, as stated previously, work is being done to address their security. In addition, the Information Analysis and Infrastructure Protection (IAIP) Directorate in DHS does work closely with DOE and with the Energy Sector owners and operators on operational security issues and the Border and Transportation Security (BTS) Directorate in DHS works with the Department of Transportation to ensure that the Nation's pipelines are safe and secure.

QUESTIONS SUBMITTED BY SENATOR PETE V. DOMENICI

SCIENCE AND TECHNOLOGY FUNDING

Question. Secretary Ridge, the Department of Homeland Security has a significant research budget to develop new technologies to secure the United States against terrorist attacks. I know that the Department has made significant progress in setting up the mechanisms to allocate science and technology funding to industry, universities, and national laboratories. This is a vital mission of your Department.

I understand that the Department is still in the process of allocating fiscal year 2003 science and technology funding. What is the current time line for completing this allocation of funding?

Answer. The Science and Technology Directorate has "execution plans", that is identified scope of work, for all remaining fiscal year 2003 funds and fully expects to have all remaining funds allocated by the end of fiscal year 2004.

Question. The Department is now engaged in the allocation of fiscal year 2004 science and technology funding. How do you plan to allocate fiscal year 2004 funding in a more timely manner?

Answer. The Department of Homeland Security has existed now for just over a year. Like the rest of the Department, the Science and Technology Directorate has been working hard to develop effective and efficient procedures and policies, including those necessary for selection of performers of the work to be done and the subsequent contractual processes and allocation of funds. As these procedures get established, projects will be awarded and funded in a more timely manner. I am pleased to say that in the last 3 months, the Science and Technology Directorate has made significant progress in allocating its available funding into the hands of those researchers who are developing and transitioning the vital technologies and tools to make the Nation safer. Both the Under Secretary for Science and Technology and I will continue to monitor the status of project selection and funding, and expect to see continued progress.

Question. I note that this year, the Department's budget submission is improved over last year as one would expect. Although there are security considerations, could you describe your plans to ensure transparency in the Department of Homeland Security budget? Both the Departments of Defense and Energy make their supporting budget documents public. Will you follow suit?

Answer. The Science and Technology Directorate prepares its annual Congressional Justification in an open and unclassified manner and will continue to do so as long as programs do not move into the sensitive realm. In addition, the Science and Technology Directorate prepares its written testimony for the record for each

of its budget-related hearings in an unclassified document. This written testimony contains the supporting documentation for its budget request and becomes publicly available.

Question. One of the biggest challenges in the science and technology area has to be coordinating the allocation of funding between near-term and applied technology and basic, long-term R&D funding.

What level of coordination is being provided by your office, Mr. Secretary, to ensure an appropriate split between near-term and long-term R&D?

Answer. I have delegated the responsibility for determining the appropriate split between near-term and long-term research and development to the Under Secretary for Science and Technology and he keeps me and others informed, although the final responsibility is mine. In the approximately 1 year 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 the Science and Technology Directorate's expenditures in basic research, applied research, and development to date, excluding construction funding.

SCIENCE AND TECHNOLOGY DIRECTORATE R&D INVESTMENTS

[In millions of dollars]

Fiscal year	Fiscal year 2003 (actual)	Fiscal year 2004 (estimated)	Fiscal year 2005 (proposed)
Basic	47	117	80
Applied	59	56	229
Developmental	398	608	643
Total	504	781	952
Percent 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. In addition, the Science and Technology Directorate is allocating a portion of its resources to high-risk, high-payoff technologies and expects to gradually increase its investments in long-term research and development to a level appropriate for its mission and the Department.

Question. What do you envision as the role of the Department of Homeland Security in investments in future R&D to meet homeland security requirements?

Answer. At the current time, the Science and Technology Directorate is working hard with available funds to fill critical gaps in our Nation's ability to prevent, protect against, respond to and recover from potential terrorist attacks; however, we are all well aware that it is only with a strong investment in long-term research that we can feel confident we are maintaining a robust pipeline of homeland security technologies to keep us safe for the decades to come. Successful businesses reinvest 10–15 percent of their total budget in research and development; the Science and Technology Directorate will strive in future years to invest a similarly significant portion of its resources into long-term research.

INTERAGENCY COLLABORATION

Question. Mr. Secretary, the Department of Homeland Security combines the programs and personnel for many Federal agencies. Creating a culture as one department is a real challenge, but there are capabilities throughout the Federal Government that can assist your Department in meeting homeland security threats.

I would encourage the Department to develop strong positive relationships with other Federal departments and agencies where there is opportunity for collaboration and cooperation to make your job easier.

Is it correct that your Department has worked with both the Department of Energy and the National Nuclear Security Agency (NNSA) as it develops its programs to meet homeland security threats?

Answer. The Department of Homeland Security has worked very closely with the Department of Energy (DOE) and NNSA from the very early stages of the development of the Science and Technology (S&T) program. The DOE laboratories provided extensive technical expertise and advise regarding the S&T program development.

Question. How would you characterize these interactions?

Answer. The Department's interactions with DOE and NNSA have been very positive. The Department of Homeland Security's (DHS's) S&T staff has an open communication relationship with DOE senior managers as well as with the DOE field personnel. Since some of the S&T staff came from DOE, there are close ties and good relationships that facilitate developing the processes of how DOE and DHS work together. When issues arise, they are quickly elevated so that communication occurs between the appropriate parties in both Departments and a resolution achieved.

Question. What potential do you see for future collaborations?

Answer. The Department of Homeland Security fully expects to continue and enhance its collaborations with the DOE and NNSA, as well as other Federal agencies conducting work of relevance to homeland security. For example, the S&T Directorate is committed to utilizing the extensive capabilities of all DOE laboratories and to engage them in all aspects of our research, development, testing and evaluation (RDT&E) program. The Directorate's Office of Research and Development is developing an enduring RDT&E capability through stewardship of the homeland security complex. To meet the Federal stewardship goal, the DOE laboratories will play a significant role in assisting in the strategic planning of the threat-based programs such as radiological/nuclear and biological countermeasures programs. The DOE laboratories also have significant existing capabilities and facilities for addressing terrorist threats, thus DHS will contribute support for some existing DOE facilities and reach-back into these unique capabilities. In addition, the DHS University Scholars and Fellows program is working with the DOE laboratories to place students with DOE mentors.

Question. The science and technology directorate at the Department has had discussions with the DOE national laboratories in such areas as radiological and nuclear and bioterrorist threats. The labs have significant capabilities to assist the Department of Homeland Security. Do you envision these collaborations continuing? Are there any barriers to such activities? If so, can Congress assist in addressing these issues?

Answer. The Department's Science and Technology Directorate will continue to utilize the DOE laboratories to address S&T requirements including key threat areas such as radiological, nuclear and biological countermeasures. Collaborations between DHS and DOE have been very successful to date, and the Science and Technology Directorate plans to continue these collaborations well into the future. There are currently no barriers to these collaborations. If circumstances change, the Department will bring this to the attention of Congress.

QUESTIONS SUBMITTED BY SENATOR BEN NIGHTHORSE CAMPBELL

Question. Over the last couple of years, I have worked to provide funding to the Federal Air Marshals (FAMs) for an in-flight communications system. I believe that this system would provide the FAMs with the communications they need to safeguard our airlines and the millions of passengers who fly on them each year.

I know that you are constantly going through reorganizations over at DHS and I have learned that the Office of Science and Technology may be proceeding to equip only those airlines that already have seatback phones with these communications for the FAMs.

But it is my understanding that many airlines do not have seatback phones. How can we ask Americans to fly on these airlines if they don't have the same level of security that is being provided to others?

Answer. Current Status. With reference to "may be proceeding to equip only those airlines that already have seatback phones with these communications for the FAMs", the Federal Air Marshal Service (FAMS) currently has access to the commercially available Verizon Airfone service, only when FAMs fly on aircraft with such a system installed. Recent statistics indicate that this system is installed on approximately 40 percent of the aircraft on which FAMs fly. This limited access includes voice only, via a tethered handset and does not provide for data, wireless, or pre-emption of service during an emergency situation. While the FAMS will conduct tests utilizing this technology, additional testing will be performed on other developing technologies with other service providers.

Phase I—Commercially Available Field Evaluation

The Federal Air Marshal Service is on the verge of conducting a field evaluation, which will focus on foundational and component testing; as well as, evaluation of FAMS applications over a commercially available communication system.

The foundational testing will seek to determine the most appropriate wireless communication protocol(s) for the FAMS to use for the Air-to-Ground Communication System (AGCS). This test will look at IR (infra-red), RFs (radio-frequencies), 802.11x, and Bluetooth technologies. The test will evaluate all of the technical and security aspects of the protocols, as well as aviation related aspects such as, compatibility with aircraft systems. General market trends and industry's development of wireless communications protocols will also be studied.

The component testing will seek to evaluate the transmission and reception of voice and data across an existing commercially available communication system, and measure the ability of the system to handle the current FAMS applications—including the Surveillance Detection Report and other applications.

AGCS Strategic Planning

Additionally, the FAMS has been working in concert with the Department of Homeland Security, Science and Technology, to rigorously identify the needs, scalability, and interoperability of the future AGCS. As a result of joint efforts of DHS S&T and the FAMS, an AGCS strategic plan is scheduled to be completed in September 2004.

AGCS Working Group

At the request of Congress in HR 108–169, the FAMS is chairing an AGCS Working Group to develop a technical implementation plan, as well as, develop a business/government partnership for the implementation of this system.

To date, the FAMS have hosted two working group meetings, which were attended by: National Aeronautics and Space Administration (NASA), Glenn Research Center; Federal Aviation Administration (FAA), NEXCOM (Next Generation Communications) and FAA GCNSS (Global Communication, Navigation, and Surveillance System); the JPDO (Joint Planning and Development Office); U.S. Special Operations Command; U.S. Northern Command/NORAD/CONR; United States Air Force; Department of Homeland Security; and others.

Milestones

January 2003.—Air to Ground Charter signed by Adm. Loy, then TSA Administrator.

Jan-Mar 2003.—FAMS participate in multiple air to ground demonstrations.

September 2003.—FAMS managed services provider selected, work begun on air to ground field evaluation.

November 2003.—Managed services provider issues RFP's for AGCS field evaluation.

December 2003.—RFPs returned, scored—recommendations made.

April 2004.—FAMS issues AGCS field evaluation final recommendation. DHS S&T begins working with FAMS on long-term strategic planning. NASA offers strategic alliance with FAMS.

May-August 2004.—AGCS field evaluation conducted.

July 2004.—Aviation and communications industries invited to review draft AGCS strategic plan and participate in AGCS Working Group

September 2004.—AGCS Strategic Plan briefed to Congress

September 2004.—AGCS Strategic Plan completed.

Goals to be achieved

—FAMS finalize contract modifications in order to move forward on field-testing and evaluation.

—Attain FAA approval for FAMS in-flight wireless communications protocols.

—Attain FCC approvals for same, focusing on aviation and broadband technologies.

—Attain Airlines approval and determine investment strategy for in cabin-aviation communication (AGCS) system(s).

—Complete FAMS AGCS strategic plan.

—Agency review of field evaluation recommendations.

Program Summary.—The FAMS is evaluating currently installed technology for immediate application and use by operational FAMS while continuing to pursue a long-term solution to FAMS AGCS needs, which may include developing technologies not associated with current in-flight communications. This long-term solution is encompassed by the AGCS Working Group, law enforcement and aviation communities and promotes confidence in our Nation's civil aviation system to detect,

deter and defeat hostile acts targeting U.S. air carriers, airports, passengers, and crews.

SMALL BUSINESS CONTRACTING

Question. As I said in my statement, Colorado is home to a number of small companies that have developed cutting edge technologies to keep not only us safe, but law enforcement officials and first responders safe as well.

I am just curious as to the number of small companies, those with 100 or less employees, that you are working with to provide us with their technology?

Answer. The Small Business Innovation Research (SBIR) Program defines a small business as one with 500 employees or less. At the time of contract award, DHS determines if the winner is a small business under this size criterion, as well as checking other criteria of the program such as U.S. ownership, location in the United States, employment of principal investigator, etc. DHS does not keep records of actual company size under 500 employees.

The first DHS SBIR solicitation requested proposals from small businesses in eight topic areas. Altogether, 374 responses were received and 66 were selected to enter negotiations for contract award in the first Phase. Three of these businesses are located in Colorado.

Question. What percentage of your procurement dollars is being awarded to small businesses?

Answer. The Small Business Innovation Research (SBIR) program is funded at 2.5 percent of extramural R&D funds. This equates to \$19.6 million in fiscal year 2004 for the Small Business Innovation Research Program, all with small businesses. In addition, small businesses are participants in our open solicitations, such as the one issued last fall for Detection Systems for Biological and Chemical Countermeasures. Among the 40 winning individual companies (or their teammates) in that fully competitive, \$76 million solicitation, there were 35 small businesses.

Question. How do you define what is a small company?

Answer. DHS uses the SBIR definition of 500 employees or less.

Question. Can you discuss with me where we are with liability protections for all contractors?

Answer. As part of the Homeland Security Act of 2002, Public Law 107-296, Congress enacted the several liability protections for the sellers of anti-terrorism technologies. The Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act) provides incentives for the development and deployment of anti-terrorism technologies by creating a system of risk and liability management. The purpose of the SAFETY Act is to ensure that the threat of liability does not deter potential manufacturers or sellers of anti-terrorism technologies (ATT) from developing and commercializing technologies that could significantly reduce the risks or mitigate the effect of large-scale terrorist events. Therefore, the SAFETY Act creates certain liability limitations for "claims arising out of, relating to, or resulting from and act of terrorism" where a qualified anti-terrorism technology (QATT) has been deployed. The SAFETY Act does not limit liability from harms caused by an anti-terrorism technology when no act of terrorism has occurred.

The definition of a qualified anti-terrorism technology is very broad and includes products, equipment, services (including support services), devices, or technology (including information technology) that is designed, developed, modified, or procured for the specific purpose of detecting, identifying, preventing, or deterring act of terrorism, or limiting the harm that such acts might otherwise cause.

Sellers of ATTs may apply for SAFETY Act protection on line at www.safetyact.gov, or they may submit their application electronically or in hard copy. Each application will be reviewed in accordance with the criteria set forth in the SAFETY Act to assess its technical capabilities and to determine if SAFETY Act protection is necessary in order to deploy the technology more broadly. To date there are 19 full applications in various stages of review as well as 61 pre-applications. The pre-application process is optional and is designed to provide early feedback to the applicant regarding whether the technology would be considered for SAFETY Act protection.

QUESTIONS SUBMITTED BY SENATOR LARRY CRAIG

Question. I believe that you have heard from Members of Congress from Illinois, New York, and Idaho about their concerns in excluding DOE national laboratories in those three States from playing on the same field as your designated "intra-mural" laboratories. I was under the impression that DHS had understood Congress's desire in creating your department, that DHS would approach the DOE

national labs on a level playing field. When visiting with you prior to your confirmation, I had felt I had your assurance to that effect.

I have made clear to you my concerns about the process your office used in establishing the intramural/extramural laboratory system. I have concerns about the validity of this approach and its outcome for both the country and the extramural laboratories. These concerns include: The reduced ability of DHS to bring the best talents and capabilities to bear on some of our most significant national security threats. The practicality and propriety of setting up a system that not only encourages, but requires the extramural laboratories to compete against industry and universities in order to contribute to the solutions of important homeland security challenges. This is of particular concern since the work designated for HSARPA and SED is work that your staff has already indicated can be performed without unique capabilities that exist in the national laboratories. The thin reasoning and basis that has been put forward by DHS as a rationale for selecting the intramural labs just doesn't appear to hold up.

Please provide the precise criteria used for selection of intramural and extramural labs. Also provide the explanation of why Argonne National Lab, Brookhaven National Lab, and Idaho National Engineering and Environmental Lab do not meet the criteria for being intramural laboratories.

Answer. The Department of Homeland Security, through Section 309 of the Homeland Security Act of 2002, is provided access to the national laboratories and sites managed by the Department of Energy to carry out the missions of DHS.

The DHS Science and Technology Directorate, wishing to make the best use of each of these laboratories and sites in consonance with statute, regulation, and policy, asked laboratories and sites to make a decision regarding their desired mode of interaction with the Directorate—to participate in S&T's internal strategic planning and program development processes, or, if otherwise permissible under applicable law, regulation, contract, and DOE policy, to respond to certain types of S&T solicitations open to the private sector.

On March 31, 2004, the following national laboratories and sites communicated their decision to Under Secretary McQueary to participate in S&T's internal strategic planning and program development processes: Argonne National Laboratory, Bechtel Nevada, Brookhaven National Laboratory, Idaho National Engineering and Environmental Laboratory, Lawrence Livermore National Laboratory, Los Alamos National Laboratory, Oak Ridge National Laboratory, Pacific Northwest National Laboratory, and the Sandia National Laboratories.

A consequence communicated to the national laboratory directors in advance of their decision is that, as a result of such participation, a national laboratory will be ineligible to participate in open solicitations to the private sector for a period of 3 years after it ceases engagement in the S&T strategic planning and program development processes.

S&T will give the laboratories access to internal DHS strategic planning information. DHS policy is that if any non-DHS entity, including a national laboratory, receives that kind of information, DHS considers that entity to have an "organizational conflict of interest" that makes the entity ineligible to participate in any solicitations open to the private sector issued by S&T.

Question. Do you think that it is appropriate for national labs to be in direct competition with universities and industries for HSARPA work?

The Homeland Security Advanced Research Projects Agency (HSARPA) solicitations seek to the maximum extent possible to capture the best ideas and solutions. To achieve this end, Broad Agency Announcements (BAAs) are used. Under a BAA, teams are not in direct competition; each team is judged on the basis of the unique ideas proposed to solve the broadly defined technology challenge. DOE Order 481.1B provides the guidance DOE uses for the national laboratories regarding participation in BAAs with universities and industries.

The DHS Science and Technology Directorate, wishing to make the best use of each of these laboratories and sites in consonance with statute, regulation, and policy, asked laboratories and sites to make a decision regarding their desired mode of interaction with the Directorate—to participate in S&T's internal strategic planning and program development processes, or, if otherwise permissible under applicable law, regulation, contract, and DOE policy, to respond to certain types of S&T solicitations open to the private sector.

On March 31, 2004, the following national laboratories and sites communicated their decision to Under Secretary McQueary to participate in S&T's internal strategic planning and program development processes: Argonne National Laboratory, Bechtel Nevada, Brookhaven National Laboratory, Idaho National Engineering and Environmental Laboratory, Lawrence Livermore National Laboratory, Los Alamos

National Laboratory, Oak Ridge National Laboratory, Pacific Northwest National Laboratory, and the Sandia National Laboratories.

A consequence communicated to the national laboratory directors in advance of their decision is that, as a result of such participation, a national laboratory will be ineligible to participate in open solicitations to the private sector for a period of 3 years after it ceases engagement in the S&T strategic planning and program development processes.

Should we assume that cost will not be a primary factor in selecting winners for HSARPA and SED contracts? If it is a primary factor, do you expect any national laboratories to be able to compete on a cost basis?

Answer. The Homeland Security Advanced Research Projects Agency (HSARPA) and the Office of Systems Engineering and Development (SED) consider other criteria, such as technical approach, performance improvement if successful, value to the DHS user, program management strategy, and capabilities of researchers to perform proposed work, more important than the total cost of the research. The S&T Directorate looks at the total cost of the research to confirm that it is reasonable, but it is only a deciding criterion if the costs are too high or too low. The eventual cost of the fielded system and its operation are frequently considered under the value to DHS user criterion; this should differ by technical approach, but not by category of proposer.

Costs can also enter the final evaluation of proposals in a determination of “best overall value to the government.” Under best value, all factors are simultaneously evaluated looking to create out of the family of selected proposals the best diversified programmatic solution for the government against the total available funding.

S&T program solicitations seek to the maximum extent possible to capture the best ideas and solutions. To achieve this end, Broad Agency Announcements (BAAs) are used. Under a BAA, teams are not in direct competition; each team is judged on the basis of the unique ideas proposed to solve the broadly defined technical challenge.

Question. Wouldn't it be reasonable to have a system where all of your critical R&D requirements were met through competitive processes in order to assure access to the broadest array of talent in a cost efficient way? Do you believe that this is what Congress intended?

Answer. DHS recognizes the unique talents at each of the DOE national laboratories, and is committed to maximizing opportunities for all the DOE laboratories in support of homeland security. We believe that by allowing the national laboratories to support S&T either through programmatic partnerships or project-based work, maximum efficiency in resource utilization may also be achieved.

S&T conducts full and open competitions for a majority of its research, development, testing and evaluation programs through Broad Agency Announcements. The Office of Research and Development will continue to conduct performance-based work with the national laboratories.

Question. Knowing that Congress debated and rejected proposals for folding one or more national labs into DHS when it was creating the new department, under what authority does DHS now proceed with this same concept, but administratively instead of legislatively?

Answer. 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 laboratories and sites and provided for access to them in support of the Department's mission.

The existing DOE laboratories have 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 and 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.

QUESTIONS SUBMITTED BY SENATOR ROBERT C. BYRD

R&D CONSOLIDATION

Question. The fiscal year 2005 budget request proposes to consolidate R&D budgets from the Coast Guard, Emergency Preparedness and Response Directorate, and from the Immigration and Customs Enforcement bureau. Other research budgets, such as \$154 million for the Transportation Security Administration were not included in this consolidation. What plans are there to consolidate all the Department's research budgets within the Science & Technology Directorate? If so, what is the timeline for completing the consolidation? What are the benefits of consolidating R&D budgets under one Directorate? What savings are anticipated by consolidating the Department's research budgets under one roof?

Answer. We have begun the consolidation 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. We expect to have this process completed by the end of fiscal year 2004 in accordance with the Congressional directive.

Consolidation of the research and development functions of the Department's components will significantly improve the Department's overall ability to meet its mission. With consolidation, we can ensure that operational end-user requirements and needs are being met by the best science and technology that can be brought to bear on the problem, whether that expertise comes from internal or external sources. We will be able to enhance our efforts to avoid duplication of effort in the R&D areas, and we fully expect to find synergies develop: what is created to meet the requirements of one component may be able to be fielded to support the needs—stated or not yet recognized—of another. The specific cost savings expected will be identified as part of the process of R&D consolidation.

DETECTION TECHNOLOGY

Question. When Secretary Ridge testified before the subcommittee in February, he said that if a passenger wanted to board a plane with a biological weapon, the Department does not currently have the capacity to detect it. He said that acquiring such a capability is a top priority for the science and technology directorate. How does your budget address this issue?

Answer. The Biological Countermeasures portfolio in the S&T Directorate is currently initiating systems studies to better define needs and options for detection of a biological agent release aboard an aircraft. Detection of a biological pathogen during the passenger security screening process remains a difficult problem, but we are also investigating potential detection options. It is possible that modifications to current technology can provide interim capability while the detection efforts described above can provide an improved future capability.

UNIVERSITY CENTERS OF EXCELLENCE

Question. In fiscal year 2004, Congress appropriated \$68.8 million for University programs under the Science and Technology Directorate. When Under Secretary McQueary testified on March 2, he said that the 3 centers would be selected in fiscal year 2004 and the fiscal year 2005 budget request would be sufficient to maintain three centers. How many centers would be selected in fiscal year 2004 and fiscal year 2005 if the budget request maintained the current level of funding instead of cutting the program by \$39 million?

Answer. In addition to the risk analysis and agro-terrorism centers already selected in fiscal year 2004, we anticipate two more solicitations for University-based Homeland Security Centers this fiscal year. If the fiscal year 2004 level of funding were maintained for fiscal year 2005 and beyond, an additional five Centers could be selected. SAFECOM

The budget request for SAFECOM is \$22.105 million. The Department's budget justification states that this program is a cost-share program and anticipates receiving \$12.5 million from within DHS and \$9.55 million from other Federal departments. Please provide the specific contributions from each DHS component and from each of the other Departments contributing to this program.

Question. How much was anticipated for SAFECOM in fiscal years 2003 and 2004 versus the amount reimbursed from other agencies? Please provide the specific con-

contributions from each DHS component and from each of the other Departments contributing to this program.

On February 23, the Secretary said that “the Department has identified technical specifications for a baseline interoperable communication system.” Please describe these technical specifications and how it will benefit first responders. What is the timeline to implement these specifications? What is the cost impact of these specifications? Will the Department establish a separate funding mechanism to assist first responders pay for this short-term solution?

Answer. The chart below outlines the funding for SAFECOM expected for fiscal year 2003 and fiscal year 2004, and the actual amount collected by the program in fiscal year 2003. It is the current expectation that all fiscal year 2004 funding provided by DHS is from the Chief Information Officer’s wireless account.

SAFECOM FUNDING

[In millions of dollars]

Agency	Actual fiscal year 2003 Funds Contrib- uted	Anticipated fiscal year 2004 Funds Contrib- uted
USDA	1.431	1.520
DOD	3.345	1.770
DOE	1.431	1.430
HHS	1.431	1.520
DHS	12.520
Dol	2.951
DoJ	4.312
Treasury	9.500
Total	17.138	26.023

The Department will require certain minimum specifications relating to interim interoperable solutions, such as cross-band repeaters and patching units. These specifications will allow public safety practitioners to clearly articulate what technical requirements must be met by vendors of communications equipment so that purchases made in the short term are successfully targeted at equipment that meets their immediate needs. Since many commercial units are already capable of meeting these requirements, the cost of these units should be unaffected.

The Department is still exploring options for funding and will release an implementation timeline accordingly.

GRANTS & CONTRACTS

Question. Of the funds appropriated in fiscal year 2004, provide a table that shows the number of grants provided, the amount for each grant, the recipient, and the purpose. Provide the same information for contractual agreements.

Answer. See table below.

Type	Amount	Project Title/Purpose	Performer	Procurement Agent
BAA	\$30,000,000	Technical Support Working Group, Rapid Prototyping	Multiple Awards Pending	Naval System Management Activity
BAA	6,045,395	Fund for RA 03-01, Detection Systems for Biological and Chemical Countermeasures (DSBCC), TTA-3 and TTA-5.	Multiple Awards Pending	Ft. Detrick, USAMRAA
BAA	5,710,000	Scene Understanding (NRL BAA 55-03-02 Artificial Intelligence Technologies) & BAA 55-03-05 Advanced Intelligence Technologies).	Multiple Awards Pending	Navy Research Lab
BAA	5,230,000	Threat Vulnerability, Intelligence and Information Analysis, and Warning Capabilities of DHS (BAA 04-02).	Multiple Awards Pending	Navy Research Lab
BAA	6,196,909	Detection Systems for Biological and Chemical Countermeasures (RA 03-01 TTA-4).	Multiple Awards Pending	Ft. Detrick, USAMRAA
BAA	2,070,000	Domain Name System Security (DNSSEC) (Air Force Research Lab/Information Grid System BAA 03-18-IFKA Cyber Defensive & Offensive Operations Technology).	Multiple Awards Pending	Air Force Research Lab
BAA	54,589,000	Funds for BAA 04-01 (Rad/Nuc Countermeasures Systems Architectures Analysis) and BAA 04-02 (Rad/Nuc Detection Systems).	Multiple Awards Pending	U.S. Navy Space and Air Warfare Center (SPAWAR)
BAA	2,050,000	Large Scale Network Security Test & Evaluation Datasets Program (DOI/NBC BAA 03-05-FH).	Multiple Awards Pending	DOI/NBC
BAA	10,000,000	Fund for RA 03-01, Detection Systems for Biological and Chemical Countermeasures (DSBCC), TTA-5.	Multiple Awards Pending	Ft. Detrick, USAMRAA
BAA	102,000	Evaluation Plan for BAA 04-02, Detection Systems for Radiological and Nuclear Countermeasures (DSRNC) HSARPA Review Support.	Oak Ridge National Laboratory	DOE
BAA	7,000,000	Phase II B Funding for RA 03-01, Detection Systems for Biological and Chemical Countermeasures (DSBCC) TTA-2.	Multiple Awards Pending	Ft. Detrick, USAMRAA
BAA	896,600	Live Agent Testing Evaluation (RA 03-01 TTA 3/4/5—Portable High-Throughput Integrated Laboratory Identification System, Lightweight Autonomous Chemical Identification System, Autonomous Rapid Facility Chemical Agent Monitor).	Multiple Awards Pending	Ft. Detrick, USAMRAA
BAA Total				
129,890,104				
Contract		Counter MANPADS Development and Demonstration Phase.	Awards Pending	DHS
6,000,000				

Contract	60,000	Support for Model OT Agreement Analyses	Logistics Management Institute (LMI)	DHS
Contract	4,678,601	Counter MANPADS Program Support	SRS Technologies	Ft. Detrick, USAMRAA
Contract	859,873	Operational and Support Staffing for Office of Weapons of Mass Destruction (WMDO)	ANSER Corp	DHS
Contract	208,750	Enhancing International Travel Security	Organization for Economic Cooperation and Development	Department of the Interior National Business Center/Fort Huachuca
Contract	5,058	Additional Funding for Goods Used ISO Biowatch	VWR International	CoastGuard
Contract	371,440	Bio Watch Operations Support	Booz Allen Hamilton	Department of the Interior National Business Center/Fort Huachuca
Contract	57,120	Unmanned Aerial Vehicle Analysis Support	SRA International	Department of the Interior National Business Center/Fort Huachuca
Contract	90,000	ORION—GPS Integration	Orion Electronics (Award Pending)	Department of Interior, Gov Works
Contract	900,000	Support of Civil Aviation Security Systems Engineering Study	Center for Naval Analysis Corporation (CNAC)	DHS
Contract	282,951	Programmatic and Technical Management Support to the Director, ORD	SPARTA, Inc	Ft. Detrick, USAMRAA
Contract Total		13,513,793		
Grant	3,310,826	DHS Scholarship/Fellowship Program	Oak Ridge Institute for Science and Education (ORISE)	DOE
Grant	4,000,000	University of Southern California—University Programs Grant	University of Southern California	DHS/FEMA
Grant Total		7,310,826		
RA	270,000	IDA Chemical Hazard Analysis	Institute for Defense Analysis (IDA)	DOD Washington Headquarters Service (WHS)
RA	161,998	South Florida Hawkeye Project fiscal year 2004, BTS	Coast Guard HQ	DHS/USCG
RA	1,131,679	DHS Cyber Security Testbed	UC Berkeley, USC, UC Davis, Penn State, Purdue, ICIR	National Science Foundation (NSF)
RA	2,300,000	South Florida Hawkeye Project fiscal year 2004, BTS	United States Coast Guard	DHS/USCG
RA	230,000	Study of Emerging Threats and Evolving Technologies	Institute for Defense Analysis (IDA)	DOD Washington Headquarters Service (WHS)
RA	390,750	Recognizing Emotion in Speech	Columbia Univ	National Science Foundation (NSF)
RA	382,500	Automated Intent Determination (Autoid)	Dr Mark Adkins, Univ of Arizona	Department of the Interior National Business Center/Fort Huachuca
RA	624,196	VACIS Image Processing and Projection (IPP)	SAIC	DHS
RA	64,600	Perimeter Security System	NAVSEA	NAVSEA

Type	Amount	Project Title/Purpose	Performer	Procurement Agent
RA	500,000	Border Gateway Protocol (BCP) Security Analysis and Evaluation of Large Scale BGP Attacks.	National Institute of Standards and Technology (NIST).	National Institute of Standards and Technology (NIST)
RA	2,500,000	Surveillance—RODS Decision Enhancements for The BioWatch System.	RODS—U of Pitt	NAVSEA
RA	3,000,000	Surveillance—ESSENCE Implementation of ESSENCE Biosurveillance Systems.	Johns Hopkins	NAVSEA
RA	200,000	Technical Advisory Group (TAG) to HSRPA on Bioerosol sensor testing and evaluation methodology.	Multiple Awards Pending	Edgewood Chemical and Biological Center
RA	10,853,444	PSITEC, technology clearinghouse	Public Safety and Security Institute for Technology	U.S. Navy Space and Air Warfare Center (SPANWAR)
RA	390,750	Recognizing and Understanding Emotion in Speech Columbia University.	Navy Research Lab.	
RA	382,500	Automated Intent Determination (AutoID)	University of Arizona	Navy Research Lab
RA	3,450,000	Bioinformatics and Assay Development Program	Multiple Awards Pending	Ft. Detrick, USAMRAA
RA	6,000,000	Rapid Prototyping	Multiple Awards Pending	Navy Research Lab
RA	50,000	Provides funding for Evaluation Plan for BAA 04-02, Detection Systems for Radiological and Nuclear Countermeasures (DSRNC).	Sandia National Laboratory	DOE
RA	76,000	Evaluation Plan for BAA 04-02, Detection Systems for Radiological and Nuclear Countermeasures (DSRNC).	Lawrence Livermore National Laboratory	DOE
RA	6,888	Office of Weapons of Mass Destruction—Computer Equipment.	DHS/GSA Schedule	DHS
RA	2,500,000	Evaluation of a Deployed Biosurveillance System	Potomac Institute	Department of the Interior National Business Center/Fort Huachuca
RA	539,720	Port Authority NY/NJ Testbed—PNWL	Pacific Northwest National Laboratory	DOE
RA	500,000	Port Authority NY/NJ Testbed—SRTC	Savannah River Technology Center	DOE
RA	1,000,000	Port Authority NY/NJ Testbed—EML	Environmental Measurements Laboratory	DOE
RA	506,452	DHS Industry Forum	Center for Technology Commercialization (CTC)	DOJ, Office of Justice Programs
RA	412,988	Port Authority NY/NJ Test Bed PNWL: Sys Analysis	Pacific Northwest National Laboratory	DOE
RA	13,000,000	Radiological/Nuclear Test and Evaluation Complex	Bechtel Nevada	DOE
RA	175,000	Weapons of Mass Destruction (WMD) and Nuclear Assessment Training.	Camp Peary AFETA	Armed Forces Experimental Training Activity (AFETA)—Camp Peary
RA	66,570	Office of Weapons of Mass Destruction—Secure Portable Phones.	DHS	DHS
RA	5,000	DHS Facilities/GSA Support of S&T, letterhead, etc.	General Services Administration	DHS
RA	250,000	Interagency Board	Battelle supporting Interagency Board (IAB)	DHS
RA	13,244,400	Bio Watch Operations Support	Environmental Protection Agency	EPA

RA	262,500	Unmanned Aerial Vehicle Analysis of Assumption/General Services Administration.	GSA.	National Science Foundation (NSF)	National Science Foundation (NSF)
RA	41,680	Second Intelligence and Security Informatics Symposium (ISI 2004).	National Science Foundation (NSF)		
RA	2,500,000	DHS Facilities/GSA Support of S&T Relocation	General Services Administration	DHS	
RA	8,500,000	Homeland Security Institute	Award Pending	Ft. Detrick, USAMRAA	
RA	103,079	TDY Support to Chemical Countermeasures Portfolio U.S. Army Edgewood Center.	U.S. Army.		
RA	5,000,000	USCG Research & Development	U.S. Coast Guard	USCG	
RA	80,000	Point Defense Against Aircraft Attack	Institute for Defense Analysis (IDA)	DOD Washington Headquarters Service (WHS)	
RA	18,965	John Rein 90 Day Extension	NETC	Naval Education and Training Center	
RA	489,322	Strategic Planning	Award Pending	Gov Works	
RA	170,500	Professional & Engineering Services	Award Pending	Department of Interior, Gov Works	
RA	480,000	Support for Planning Documents	Touchstone Corp	Department of the Interior National Business Center/Fort Huachuca	
RA	2,601,000	Border Safe Integrated Feasibility Experiment Phase II	Corporation for National Research Initiatives (CNRI)	Department of the Interior National Business Center/Fort Huachuca	
RA	25,000	Support of International Meeting of Biometrics Experts	National Institute of Standards and Technology (NIST)	National Institute of Standards and Technology (NIST)	
RA	100,000	Enhanced International Travel Security Support	Asian Technology Information Program (ATIP)	Office of Naval Research	
RA	100,000	DHS Canada Collaboration	Sandia National Laboratory	DOE	
RA	86,400	Radiological Dispersal Device (RDD) Workshop	Sandia National Laboratory	DOE	
RA	216,250	Chemical Biological National Program (CBNP) Continuation Program—ANL.	Argonne National Laboratory	DOE	
RA	5,820,000	Chemical Biological National Program (CBNP) Continuation Program—LNL.	Lawrence Livermore National Laboratory	DOE	
RA	2,589,500	Chemical Biological National Program (CBNP) Continuation Program—LANL	Los Alamos National Laboratory	DOE	
RA	2,188,750	Chemical Biological National Program (CBNP) Continuation Program—SNL.	Sandia National Laboratory	DOE	
RA	598,875	Chemical Biological National Program (CBNP) Continuation Program—PNWL.	Pacific Northwest National Laboratory	DOE	
RA	567,500	Chemical Biological National Program (CBNP) Continuation Program—BNL	Lawrence Berkeley National Laboratory	DOE	
RA	75,000	Chemical Biological National Program (CBNP) Continuation Program—ORNL.	Oak Ridge National Laboratory	DOE	
RA	62,500	Chemical Biological National Program (CBNP) Continuation Program—INEEL.	Idaho National Engineering and Environmental Laboratory.	DOE	

Type	Amount	Project Title/Purpose	Performer	Procurement Agent
RA	4,215,475	Plum Island Animal Disease Center (PIADC)—First Quarter fiscal year 2004 Continuation Funding.	Plum Island Animal Disease Center (PIADC)	DHS
RA	10,166,544	Plum Island Animal Disease Center O&M	Plum Island Animal Disease Center (PIADC)	DHS
RA	1,060,400	Environmental Measurements Lab	Lawrence Livermore National Laboratory	DOE
RA	6,930,000	Threat Vulnerability Integration Systems Pilot (TVIS)—LNL.	Lawrence Livermore National Laboratory	DOE
RA	3,870,000	Threat Vulnerability Integration Systems Pilot (TVIS)—PNWL.	Pacific Northwest National Laboratory	DOE
RA	1,480,050	Yarrow Behavioral Analysis Technical Support Nuclear Assessment Program.	Lawrence Livermore National Laboratory	DOE
RA	250,409	PNML Support to Emergency Preparedness and Response Program.	Pacific Northwest National Laboratory	DOE
RA	800,000	Weapons of Mass Destruction—Nuclear Assessment Program (WAP).	Los Alamos National Laboratory	DOE
RA	100,000	Weapons of Mass Destruction—Nuclear Assessment Program (WAP).	Oak Ridge National Laboratory	DOE
RA	4,525,000	Nuclear Assessment Program, Credibility Assessment	Lawrence Livermore National Laboratory	DOE
RA	320,000	Nuclear Assessment Program, Forensic Tech Support	Pacific Northwest National Laboratory	DOE
RA	1,900,000	EPR Scientific Support to FEMA	Lawrence Livermore National Laboratory	DOE
RA	2,229,225	ARS Plum Island Animal Disease Center (PIADC) Scientific Support.	Plum Island Animal Disease Center (PIADC)	DHS
RA	45,980	ARS Plum Island Animal Disease Center (PIADC) Admin Support.	PLUM/Plum Island Animal Disease Center (PIADC)	DHS
RA	1,200,000	Developing a Critical Infrastructure Protection Decision Support System (CIP/DSS).	Los Alamos National Laboratory	DOE
RA	1,200,000	Developing a Critical Infrastructure Protection Decision Support System (CIP/DSS).	Argonne National Laboratory	DOE
RA	400,000	Developing a Critical Infrastructure Protection Decision Support System (CIP/DSS).	Pacific Northwest National Laboratory	DOE
RA	1,200,000	Developing a Critical Infrastructure Protection Decision Support System (CIP/DSS).	Sandia National Laboratory	DOE
RA	1,500,000	BioWatch—Orange Alert Expanded Sample Analysis	Lawrence Livermore National Laboratory	DOE
RA	1,514,000	Rad/Nuc Countermeasures—PNWL	Pacific Northwest National Laboratory	DOE
RA	3,313,000	Rad-Nuc Countermeasures PEP—LANL	Los Alamos National Laboratory	DOE
RA	101,900	NRC Workshop Conference	National Research Council (NRC)	DOE
RA	700,000	Advanced Scientific Computing—SNL	Sandia National Laboratory	DOE
RA	4,776,000	Advanced Scientific Computing—LNL	Lawrence Livermore National Laboratory	DOE
RA	85,811	Advanced Scientific Computing—ORNL	Oak Ridge National Laboratory	DOE

RA	2,500,000	National & Regional Visual Analytics Centers	Pacific Northwest National Laboratory	DOE
RA	250,000	Environmental Measurements Laboratory Second Qtr Funding for fiscal year 2004.	Environmental Measurements Laboratory	DOE
RA	1,298,500	CBNP fiscal year 2003 Continuation and New Start Funding.	Los Alamos National Laboratory	DOE
RA	4,833,500	CBNP fiscal year 2003 Continuation and New Start Funding.	Lawrence Livermore National Laboratory	DOE
RA	1,500,000	Photofission-Based Nuclear Material Detection and Characterization.	Idaho National Engineering and Environmental Laboratory.	DOE
RA	1,600,000	(Tri-Lab) Threat-Capability Assessments—LANL	Los Alamos National Laboratory	DOE
RA	1,600,000	(Tri-Lab) Threat-Capability Assessments—LINL	Lawrence Livermore National Laboratory	DOE
RA	1,600,000	(Tri-Lab) Threat-Capability Assessments—SNL	Sandia National Laboratory	DOE
RA	15,300,000	First Responder CBRNE Protective and Operational Equipment Standards Development Program.	National Institute of Standards and Technology (NIST).	DHS
RA	280,000	RADNUC Attribution Advisor	Lawrence Livermore National Laboratory	DHS
RA	255,000	Border Safe Phase II	SPAWAR	DHS
RA	2,257,098	Plum Island Animal Disease Center (PIADC) O&M Services Contract—Remainder of funding.	Plum Island Animal Disease Center (PIADC)	DHS
RA	1,199,370	ORISE Merit Review for HS Centers	Oak Ridge Institute for Science and Education (ORISE).	DOE
	186,199,518			
	17,170,000	Small Business Innovation Research Program (SBIR)	Multiple Awards Pending	Department of the Interior National Business Center/Fort Huachuca
SBIR	17,170,000			
	17,170,000			

QUESTION SUBMITTED BY SENATOR DANIEL K. INOUE

Question. I continue to have constituent businesses contact my office to ask for information about grant opportunities from the Department of Homeland Security. My staff has requested a briefing from the Science and Technology Directorate. However, the requested briefing has so far not been provided. Upon researching on the website, my staff came upon an invitation to attend a Department of Homeland Security Industry Forum. Mr. Chairman, I request that a copy of this notice be placed in the record.

I would like to quote from this announcement:

This two-day forum will provide industry the opportunity to hear, first-hand, what technology needs and requirements DHS will have in the coming years. DHS staff will provide detailed briefings on technology R&D and T&E requirements for the Department, as well as, where and when to apply for DHS funding.

A brief itinerary and list of speakers, including several members of your staff, is attached. This sounds like a great forum that my staff and constituents would be interested to attend. However, a list of registration fees is also included. The fees range from \$425 for members of the government to \$625 for private industry. I was surprised to learn of the high cost to attend this government briefing. Why are government employees required to pay \$425 to learn about these funding opportunities? Why is DHS charging other entities for this information?

Answer. Fees for this conference were maintained at levels as low as we believed feasible. In accordance with standard government practice, fees were set to help offset the costs of conducting a public forum rather than supporting the conference with public funds.

 QUESTIONS SUBMITTED TO INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION

QUESTIONS SUBMITTED BY SENATOR THAD COCHRAN

BIODEFENSE COUNTERMEASURES (BIOSHIELD)

Question. The President's budget proposes to transfer the Strategic National Stockpile back to the Department of Health and Human Services but not project BioShield. IAIP's role in the project BioShield is to make the threat assessments necessary to determine proper BioShield investments which is the rationale for the Department of Homeland Security having responsibility for this program.

What assessments have been carried out by Information Analysis and Infrastructure Protection of our vulnerabilities to biological attacks to guide decisions as to the investments which should be made to develop, produce and pre-purchase vaccines or other medications from BioShield?

Answer. The Department of Homeland Security has been assigned a role in several bioterror initiatives. One such initiative, Project BioShield, specifies DHS work with the Department of Health and Human Services (HHS) and several other Federal agencies to ensure resources are available to combat a sudden chemical or biological attack. The central premise for this program is the government must prepare for such attacks by acquiring the best vaccines/drugs for pathogens such as smallpox, anthrax and botulinum toxin. To do so, current Project BioShield guidelines require DHS evaluate likely biological/chemical threats and identify promising bio-research R&D to best address such an attack.

DHS is currently involved in an initiative designed to protect the Nation against bioterrorism. This initiative, known as the Bio-Surveillance Program, has been in operation since 2003. This program not only enhances on-going surveillance in areas such as human health, hospital preparedness, State and local preparedness, vaccine research and procurement, animal health, food and agriculture safety and environmental monitoring but will integrate these data streams with intelligence data in a comprehensive fashion.

IAIP's role in the Bio-Surveillance Program is developing a real-time system for harvesting data on the health of our population, animals, plants, and food supply, as well integrating this information with environmental monitoring and intelligence data. This integration can enable better decision-making and a more rapid Federal, State, and local response. Coordination between DHS and the Department of Health and Human Services and the Department of Agriculture is ongoing. This data exchange will help DHS, HHS, and other Federal agencies evaluate potential health threats and guide bioterrorism preparedness resource investments.

CYBER SECURITY

Question. The National Cyber Security Division, as part of the Information Analysis and Infrastructure Protection Directorate, recently unveiled the National Cyber Alert System which intends to deliver information to home computer users and technical experts in business and government agencies to better secure their computer systems from the latest computer viruses.

What progress has been made by the National Cyber Security Division to prevent the spread of this computer virus as well as future virus and worm outbreaks?

Answer. The lynch pin to preventing the spread of computer viruses and worm outbreaks is a robust and mutually beneficial relationship with the private sector. Cyber security is often a reactive process because the initiative rests with hackers and malicious agents. Developing and maintaining a partnership with the private sector is therefore a crucial means to both responding quickly to emerging threats and taking proactive measures to forefend against potential threats. The DHS/US-CERT Partner Program is composed of members that recognize their responsibility to their organizations and the Nation to improve the current and future state of cyber security. Members collectively and individually realize the need to take action and abide by principles and practices that are appropriate as critical infrastructure operators, communities of interest, vulnerability researchers, educators, and software vendors. The Partner Program consists of participants from various sectors of the cyber community who must agree to meet certain criteria in order to achieve the designation of DHS/US-CERT partner. These criteria are designed with the aim of preventing occurrences such as the spread of computer viruses and worms and other malicious activities.

Another important tool for the prevention of worms and viruses is the National Cyber Alert System. Americans are exhibiting a keen interest in the alert system. On day one of the National Cyber Alert System launch, we had more than one million hits to the US-CERT website. Today, more than 250,000 direct subscribers are receiving National Cyber Alerts to enhance their cyber security. Through the alert systems, Americans are able to receive information that is accurate and actionable. It is our goal to inform the public about the true nature of a given incident, what the facts are, and what steps they can and should take to address the problem. The offerings of the National Cyber Alert System provide that kind of information. To date, we have issued seven security tips, six security bulletins, ten technical alerts, and six non-technical cyber alerts in response to cyber security incidents through the National Cyber Alert System. We strive to make sure the information provided is understandable to all computer users, technical and non-technical, and reflect the broad usage of the Internet in today's society. As we increase our outreach, the National Cyber Alert System is investigating other vehicles to distribute information to as many Americans as possible.

Question. What is the relationship of the National Cyber Security Division with the Terrorist Threat Integration Center (T-TIC) on combating computer viruses by terrorists?

Answer. NCSA, in partnership with DHS/IAIP/IA works intensively with the law enforcement and intelligence communities including the TTIC in order to develop a comprehensive threat, risk, attribution assessment and response capability.

Question. What law enforcement agency has primary jurisdiction in enforcing cyber crimes?

Answer. No single law enforcement agency has primary jurisdiction in the investigation of cyber crime. The FBI and Secret Service are the most visible, pervasive agencies, but other organizations, such as the IRS' Office of the Inspector General or ICE's Cyber Smuggling Division, have specialized areas of responsibility in the areas of enforcing cyber laws.

HOMELAND SECURITY ADVISORY SYSTEM

Question. The Homeland Security Advisory System has evolved from a nationwide threat level status to more specific targeted areas since the latest threat level decrease in January. While the threat level is currently at an "Elevated Condition", or code yellow, specific cities and the aviation sector remain at the "High Condition", or code red. This more targeted threat level status helps focus limited resources on the most credible threat areas and at the same time allows law enforcement and first responders in other parts of the country to "stand down" while remaining vigilant. In recent testimony, Secretary Loy testified that the Department was "very close" to unveiling a system that would allow specific threat warnings to about a dozen economic sectors.

With the improvement of intelligence that has included detailed specific terrorist threats for certain metropolitan areas and specific sectors of industry, what further enhancements do you envision for the Homeland Security Advisory System?

Answer. With each raising and lowering of the Homeland Security Advisory System (HSAS), the Department of Homeland Security learns new lessons and improves its notification process. As the system has evolved, it has come to reflect the need for certain metropolitan areas and/or specific areas of industry to be notified at different times or at different levels than others. As such, DHS has become adept at providing information to such specific audiences as states and sectors through Homeland Security Information Bulletins and Advisories. Additionally, Department officials speak personally with representatives and officials of threatened States and industries, when the need arises. This personal communication, along with the ability of the system to allow DHS to communicate to certain areas what their alert level should be embody the enhancements that have been needed this far.

Question. Are you looking to enhance or improve upon any of the eight existing Federal warning systems that are currently being operated nationwide?

Answer. Yes. With the \$10,000,000 provided to IAIP in last year's Homeland Security Appropriations Conference Report (108-280) we plan to enhance and upgrade NOAA Weather Radio and the Emergency Alert System (EAS), and possibly other systems. A few vital efforts have been identified for immediate funding. Those include improving the coverage and survivability of the EAS by (1) installing a satellite-based message delivery capability and (2) by adding EAS stations to all 50 States (to include State Emergency Operations Centers) and U.S. territories. Also, there are pilot projects planned to: (1) examine how reverse 911 can be used to help disseminate alert and warning information; and (2) demonstrate how new technologies such as digital TV broadcasts/datacasting using spectrum offered by public TV can be used to improve our ability to alert the American public. These three projects represent a portion of the \$10,000,000, but the bulk of the funding will be allocated after completion of a study of available and planned alert and warning systems to develop integrated, capabilities-based architecture recommendations. This study will be completed by the end of summer.

HOMELAND SECURITY INFORMATION NETWORK

Question. Another enhancement being made by the Department in the area of information sharing is the new Homeland Security Information Network which will be able to disseminate threat information to Federal, State and local law enforcement agencies.

Is the Department on schedule to complete the first phase of the network this summer, and what is the targeted deadline to complete the flow of real-time information to all relevant end-users throughout the country?

Answer. The Department is on schedule to meet the summer deadline. We plan to begin expansion of HSIN to the county level, in conjunction with the each State's individual rollout plans, by the end of year. By the beginning of next year, we plan to be actively engaged with other homeland security partners, such as the private sector, to support further real time, secure collaborative information flow.

Question. How will the Homeland Security Information Network be different from the Joint Regional Information Exchange System and Regional Information Sharing Systems which are already in place and in use?

Answer. The Homeland Security Information Network (HSIN) is the overarching network for the Department of Homeland Security (DHS) to provide information exchange and real time collaboration between Federal, State, and municipal authorities. Within the initial program there will be four HSIN areas: HSIN/DM (Decision Maker-used by Federal, State and Urban area homeland security advisors); HSIN/EOC (used primarily by Federal, State and urban emergency operations centers); HSIN/NG (used primarily by the NGB and the State adjutant generals); and the HSIN/JRIES (used primarily by law enforcement and intelligence agencies). This summer, other areas within HSIN, like the Secret and DHSInfo areas will be activated. HSIN is the umbrella program under which all of these virtually private networks are contained.

While there is a need to be able to disseminate intelligence information across the full spectrum of the HSIN system, the primary HSIN tools to be used for intelligence dissemination will be the HSIN/JRIES (Law Enforcement and intelligence information) area and the HSIN/Secret network (JRIES at the Secret level). This will initially run on the National Guard (SIPRNet) backbone then migrate to the HSIN network once the DHS classified system becomes operational.

The goal of HSIN is to have an integrated system that uses the same tools and applications. These applications will run on separate areas of the HSIN network de-

fined by the user group's clearance, need to know, and need to act as approved by DHS.

CYBER SECURITY

Question. The Department's new initiative "Live Wire" will test civilian agencies' security preparedness and contingency planning by staging cyber attack exercises to evaluate the impact of widespread computer disruptions. Recent instances, such as the power outages in the Northeast this past August, are an example of how an attack on our critical infrastructures, such as a cyber attack by terrorists on our Nation's utility industry, could cascade across a wide region if the proper precautions are not taken immediately.

What was learned from previous simulated terrorist attacks on the Nation's cyber infrastructure, and how will "Live Wire" build upon current programs?

Answer. Strategically, Livewire demonstrated the impact of a cyber-based attack on critical infrastructures. The exercise highlighted the interdependencies among our critical infrastructures and underscored the requirement for enhanced cross-sector cooperation. At the tactical level, Livewire demonstrated the need to enhance processes for communicating cyber protection information to the public and for two-way information sharing with the private sector. Livewire prompted us to enhance our vulnerability identification and reduction capabilities. This drove us to create the Cyber Interagency Incident Management Group (Cyber IIMG) to coordinate intergovernmental preparedness and response operations. It also spurred us to expand the reach of emergency communications capabilities using a technologically advanced, secure network. In addition, we launched the National Cyber Alert System as a dissemination mechanism to provide the broadest population of public stakeholders with accessible, relevant, actionable alerts and information.

Question. How do you coordinate "Live Wire" exercises with private industry to test their cyber infrastructure vulnerabilities, and what gaps in coordination have been revealed between government agencies and the private sector?

Answer. Whereas the first responder and emergency management communities have been exercising at national, regional, and local levels for many years, the cyber response community has only formed over the past decade or so. There have been very few cyber-focused exercises at any level. Efforts to coordinate an effective cyber response capability across State and local jurisdictions and economic sectors are only beginning.

The Federal Government cannot by itself defend cyberspace from current or future threats. Acknowledging this, NCSO collaborates with industry and public-sector stakeholders across the country to define, develop, and exercise the major elements of a national cyber-space security response system. Its goals for the National Exercise Program (NEP) are to:

- Sensitize a diverse constituency of private and public-sector decision-makers to a variety of potential cyber threats including strategic attack;
- Familiarize this constituency with DHS' concept of a national cyber response system and the importance of their role in it;
- Practice effective collaborative response to a variety of cyber attack scenarios, including crisis decision-making;
- Provide an environment for evaluation of inter-agency and inter-sector business processes reliant on information infrastructure;
- Measure the progress of ongoing United States efforts to defend against an attack;
- Foster improved information sharing among government agencies and between government and industry;
- Identify new technologies that could provide earlier warning of attacks;
- Sort roles and responsibilities of government agencies and industry.

NCSO's involvement in the NEP will be guided by two principles: (1) Cyber is only one element of a multifaceted NEP; cyber elements must be closely coordinated with other elements of that program to ensure efficient use of limited resources and the most effective return on exercise investments; (2) Cyber exercise elements must not be sidelined or relegated to an "afterthought" category within the NEP.

Although the NEP is the responsibility of the Office of Domestic Preparedness (ODP), the NCSO will retain overall responsibility for planning and execution of adequate cyber response exercises. The NCSO shall identify a NEP cyber exercise program manager, ensure adequate resources are available for cyber elements of the NEP, including personnel, define NEP cyber exercise objectives and metrics, prioritize NEP cyber exercise events, solicit Federal agency and department participation in cyber-focused elements of the NEP, and initiate or approve Statements of Work for contracted cyber exercise activities.

Wherever appropriate, the NCSO will coordinate ODP on funding and personnel issues.

The NCSO requires a set of cyber-focused exercises that build grassroots cyber response capabilities quickly while also elevating the concept of strategic cyber attacks and maturing a national cyberspace security response system capable of dealing with them. Cyber-focused exercises must include a series of regularly scheduled "Building Block" exercises followed by a culminating, nationally scoped exercise similar to Livewire, also the continuation of tabletop events hosted by the USSS (Electronic Crimes task Forces).

We also require that cyber be included as an important element in targeted NEP events that do not have a cyber focus. Examples are TOPOFF, FEMA (EP&R) readiness exercises, and policy-focused seminars for senior officials. Each of these exercise events should include cyber scenarios and cyber responders.

NATIONAL CRITICAL INFRASTRUCTURES

Question. Recently published was the interim final rule for the voluntary submission of critical infrastructure information by private industry to the Department of Homeland Security with assurances that the proprietary data submitted would be safe from public disclosure.

What level of cooperation with private industry do you anticipate as you gather information on the Nation's critical infrastructures?

Answer. It is difficult to forecast the extent to which private industry will voluntarily share critical infrastructure information with DHS. We only know that private industry has consistently stated in the past that two barriers to sharing information with the government were concerns that (1) the information would be released to the public under the Freedom of Information Act and (2) the disclosure could create a civil liability for the company sharing the information. The Critical Infrastructure Information Act of 2002 and the Interim Final Rule which implements it, we believe, removes these two barriers to information sharing with the government.

Question. How will the publishing of this rule help the Department in its effort to safeguard the country's privately-held critical infrastructures?

Answer. The CII Act and implementing regulations provide private industry assurances that critical infrastructure information they voluntarily share with the government will be protected from release to the public and from use in civil litigation. We believe the PCII Program will enable the Department to receive critical infrastructure information that would not have previously been available to the government, thereby allowing for a better understanding of threats.

Question. What incentive is there for private industry to volunteer information to the Federal Government?

Answer. Private industry realizes they can assist in efforts to improve homeland security by volunteering information. What was needed was a means for them to share information that is usually considered proprietary and shielded from competition here and abroad. With the protection from FOIA disclosure offered by the CII Act, we believe the private sector can now share sensitive and confidential information that we can be analyzed to identify threats and vulnerabilities. Such analysis will provide the basis not only for developing measures to deter the threats and mitigate the vulnerabilities to which the critical infrastructure is exposed, but also for improving Federal, State, and local governments' emergency preparedness posture to respond to any attacks more effectively.

Question. In December of last year, a Homeland Security Presidential Directive was issued to produce a comprehensive, integrated National Plan for Critical Infrastructure and Key Resources Protection for all Federal departments and agencies to outline national goals, objectives, milestones, and key initiatives to be completed within 1 year.

With various departments and agencies previously conducting assessments of their vulnerabilities, do you believe this directive can be completed earlier than the deadline of December of this year?

Answer. The President intends that we meet the requirement to develop the NIPP by December 2004, but, given the urgency of the need, we will complete it earlier if possible.

Question. Has funding been requested in other departments' and agencies' budgets outside of the Department of Homeland Security to carry out the Presidential directive, or will the Department of Homeland Security be requested to assist other agencies in the assessment of critical infrastructures?

Answer. Under HSPD-7, Sector-Specific Agencies shall, among other things, "conduct or facilitate vulnerability assessments" of their respective sectors in accordance

with guidance provided by the Department of Homeland Security. Each department and agency will need to budget for efforts to carry out their HSPD-7 responsibilities and provide that information to the President and the Congress.

Question. The Congress made available over \$343,000,000 for Remediation and Protective Actions for fiscal year 2004 for critical infrastructure identification, to conduct vulnerability field assessments of critical infrastructures, and to create a database of vulnerabilities affecting the highest priority terrorist targets in order to develop better security measures for the protection of facilities and national assets.

What is the timeline of your Directorate for identifying our Nation's critical infrastructures, and what progress has been made in field assessments of the critical infrastructures that have already been identified?

Answer. We have built the National Asset Database (NADB). It is a comprehensive database designed to catalogue the Nation's critical infrastructure and key assets (CI/KA). The central purpose for constructing this database is to identify assets that may be attractive targets to terrorists so measures can be taken to help mitigate risk. There are now approximately 33,000 sites listed on the NADB, and DHS continues to receive additional nominees from States and territories. We view the NADB as a living database, therefore sites will be added or removed as warranted by ongoing assessments. Inputs continue to be received and from private industry as well as Federal, State and local governments.

In regards to field assessments of identified critical infrastructures, over the past 6 months DHS has conducted approximately 89 Site Assistance Visits (SAVs) for the highest priority sites and produced 25 Characteristics and Common Vulnerabilities (CCVs) reports on vulnerabilities for specific classes of CI/KA.

We anticipate completing another 74 CCVs by the end of the fiscal year and conduct any necessary SAVs.

Question. Who will retain the database of vulnerable critical infrastructures, and who will have access to it?

Answer. DHS will retain the NADB. As we receives additional input from States, territories, and other Federal agencies it will update/maintain the NADB and share asset information with other DHS entities, such as the Office for Domestic Preparedness (ODP), to help prioritize resource allocation for the implementation of protective measures to safeguard our Nation's critical infrastructure and key assets. State-specific information will also be shared with State Homeland Security Advisors as appropriate both to solicit comments and to identify State priorities. Appropriate access will be and is grant to private industry concerning their data and assets.

Question. What type of security procedures for our Nation's identified critical infrastructures have been implemented?

Answer. As priority assets are identified, we conduct risk analyses and consequence of attack analyses to help determine which sites are at greatest risk. PSD then develops plan templates and other tools to assist owners and operators in developing Buffer Zone Protection Plans (BZPPs) and site security protection plans. The BZPP helps develop effective preventive measures that make it more difficult for terrorists to conduct surveillance or launch attacks from the immediate vicinity of a possible target.

OFFICE FOR DOMESTIC PREPAREDNESS USE OF DATABASE INFORMATION

Question. In recent testimony, Secretary Ridge cited that the "maturity and growth" of the Information Analysis and Infrastructure Protection Directorate is allowing for better targeting of resources for the Office for Domestic Preparedness in the decision-making process for the distribution of grants to high threat areas across the country.

What improvements have been made over the past year by the Information Analysis and Infrastructure Protection Directorate to assist the Office for Domestic Preparedness in making sure that Federal funds are going to the areas where the threat of a terrorist attack is the greatest?

Answer. IAIP assisted ODP in the identification of a set of critical assets from the NADB that most warranted additional resources to enhance their security for fiscal year 2004. This resulted in the identification of approximately 1,700 assets onto a fiscal year 2004 list of assets warranting special attention for fiscal year 2004 funds.

Future development of the NADB and our efforts to identify and prioritize national critical infrastructure and key assets will, we believe, help us ensure the best protection of critical infrastructure and best use of Federal resources.

Question. How will the Information Analysis and Infrastructure Protection Directorate work to share information catalogued in the database of critical infrastruc-

tures with the Office for Domestic Preparedness to target grants to the country's highest threat areas?

Answer. Similar to fiscal year 2004, an analytical framework will be used to identify and prioritize assets on the expanded NADB, and this information will be shared with ODP to help develop its lists of assets that may require grant assistance in fiscal year 2005.

Intelligence capabilities 10. The President's budget proposes a \$19,300,000 decrease in funding for the Information Analysis and Infrastructure Protection Directorate in order to centrally fund the Terrorist Threat Integration Center (T-TIC) with other intelligence programs and also to centrally fund the Federal Bureau of Investigation's (FBI) Terrorist Screening Center with Department of Justice programs.

Question. Without the contribution of funding that the Department of Homeland Security currently makes to the Terrorist Threat Integration Center, do you believe that the Department will have an adequate intelligence presence in T-TIC?

Answer. Yes. The Department of Homeland Security (DHS) will provide 10 percent, or 30 personnel, to the Terrorist Threat Integration Center's (TTIC's) end goal of 300 personnel. This, as well as the close working relationship that TTIC and the DHS Office of Information Analysis (IA) have developed ensures an initial intelligence presence at TTIC.

Question. What will the Information Analysis and Infrastructure Protection's role be in the Terrorist Threat Integration Center and the Terrorist Screening Center without providing any funding of its own?

Answer. Per the explanation above, the DHS Information Analysis and Infrastructure Protection (IAIP) Directorate's role in both TTIC and the Terrorist Screening Center is the physical presence of personnel at each location. DHS analysts will inform the TTIC's work. Conversely, TTIC analysts will inform DHS' analysis. In addition to analytical personnel, DHS senior leadership will retain their presence at each center.

Question. How do you prevent a duplication of intelligence gathering and intelligence analysis with the Terrorist Threat Integration Center?

Answer. Terrorism analysis is a complex issue. It is an area where a certain amount of multiple analyses from different perspectives is preferred. To ensure no vital piece of intelligence is missed, the analysis of terrorist information is a shared responsibility.

DHS' Office of Information Analysis (IA) analytical intelligence mission is to protect the American homeland against terrorist attack. To do so, IAIP maps terrorist threats and capabilities against assessed vulnerabilities. IA also communicates information to State, local, tribal, major city, and private sector officials. TTIC's primary responsibility is the analysis of all international terrorism threat information whether collected domestically or abroad.

Question. Without a request for funding within the Department of Homeland Security for the integration of the multiple terrorist watchlists, how will the Department of Homeland Security participate in consolidating various agencies' terrorist lists?

Answer. The Department of Homeland Security is participating in the Terrorist Screening Center (TSC) through physical location of personnel in the center.

Question. Please distinguish the functions of T-TIC from the intelligence functions of the Information Analysis and Infrastructure Protection Directorate.

Answer. As a Directorate, IAIP enables, develops, and sustains the capability to continuously identify, assess, and prioritize current and future threats to the homeland, map those threats against vulnerabilities, issue timely warnings, provide the basis from which to organize protective measures to secure America, and assist in coordinating the response and restoration of critical infrastructure functions. Currently, IAIP is moving forward in carrying out our statutory responsibilities which include:

- Providing the full range of intelligence support to senior DHS leadership and component organizations and to State and local and private sector respondents.
- Mapping terrorist threats to the homeland against assessed vulnerabilities to drive our efforts to protect against terrorist attacks
- Conducting independent analysis and assessments of terrorist threats, including competitive analysis, tailored analysis, and "red teaming"
- Assessing the vulnerabilities of key resources and critical infrastructure of the United States
- Merging the relevant analyses and vulnerability assessments to identify priorities for protective and support measures by the Department, other government agencies, and the private sector

- As a full member of the Intelligence Community, the Office of Information Analysis partnering with other IC members, TTIC, law enforcement agencies, State and local partners, and the private sector, as well as DHS' components to manage the collection and processing of information involving threats to the Homeland into usable, comprehensive, and actionable information.
- Disseminating time sensitive warnings, alerts and advisories to Federal, State, local, and tribal governments and private sector infrastructure owners and operators

TTIC is an interagency joint venture of its partners. The TTIC members include, but are not limited to, the Department of Justice/FBI, DHS, CIA, National Security Agency, National Imagery and Mapping Agency, Defense Intelligence Agency, and the Department of State. Through the input and participation of these partners, TTIC merges and analyzes terrorist threat-related information, collected domestically and abroad, in order to form the most comprehensive possible threat picture, and disseminate such information to appropriate Federal Government recipients. TTIC draws on the particular expertise of its participating members—such as DHS' focus on homeland security and CIA's focus on terrorism information collected overseas—thereby ensuring that the terrorist analytic product takes advantage of, and incorporates, the specialized perspectives of relevant Federal agencies. TTIC provides comprehensive, all-source terrorist threat analysis and assessments to U.S. national leadership.

Currently, DHS representatives are located at TTIC, working day-in-day-out, participating in processing and analyzing terrorist threat-related information, developing, shaping, and disseminating TTIC products, assessing gaps in the available information, and ensuring that TTIC products reach appropriate DHS Headquarters elements. Through DHS, the necessary information, including threat descriptions, suggested protective measures, and locations of additional information, then reaches the appropriate State, local, tribal, major city and private sector officials. Analysts assigned to TTIC ensure that TTIC's work directly supports DHS' unique mission to protect the homeland. The threat information integration and analysis that is the beginning, not the end, of DHS' protective mission, will most effectively be carried out, as Congressional and other reviews have recommended, when all terrorism threat-related activities of the U.S. Government work together seamlessly.

QUESTIONS SUBMITTED BY SENATOR PETE V. DOMENICI

NATIONAL INFRASTRUCTURE SIMULATION AND ANALYSIS CENTER

Question. Mr. Libutti, the Department of Homeland Security has taken ownership of the National Infrastructure Simulation and Analysis Center, or NISAC. NISAC was developed by Sandia and Los Alamos National Laboratories to simulate and analyze various events and the cascading effects on critical infrastructure in the United States. Following the September 11th terrorist attacks, NISAC took on added importance as the Administration and Congress focused on homeland security. The fiscal year 2004 Homeland Security Appropriations Act had approximately \$23,000,000 for NISAC. Would you please give the Subcommittee the status of the allocation of the fiscal year 2004 funding?

Answer. The Homeland Security Appropriations Act of 2004 did not contain a specific line item for services to be provided by the National Infrastructure Simulation and Analysis Center (NISAC). However, the Department has set aside \$20,000,000 in October 2004 for NISAC programmatic efforts to be performed by Los Alamos National Laboratory (\$10,000,000) and Sandia National Laboratory (\$10,000,000). Some of the planned NISAC activities include chlorine industry studies, analyses of rail system and electric power disruptions, assessments of Hurricane Isabel impacts on infrastructure, port and inland waterway modeling, as well as urban infrastructure modeling.

Question. How much is in the President's fiscal year 2005 budget request to support activities by NISAC?

Answer. The fiscal year 2005 request for the NISAC is \$27,000,000.

Question. What are some of the activities envisioned in the fiscal year 2005 budget for NISAC?

Answer. NISAC fiscal year 2005 activities are expected to include expansion of the Center's developing National and Regional Tools into additional regions and cities of the Nation. Additionally, NISAC will begin developing consequence analysis and decision support tools to support the following:

- Expansion of the urban infrastructure suites models for transportation, telecommunications, water, public health and energy to additional high threat urban areas.
- Expansion of the dynamic simulation models to selected east and west coast ports.
- Expansion of the interdependent energy infrastructure simulation system.
- Expansion and testing of the waterways asset prioritization tool in concert with the U.S. Coast Guard and Army Corps of Engineers.
- Continued expert analysis and support to short term actions for the Department's primary missions using the Center's developing infrastructure models.

One of the items that transferred from the Department of Energy to the Department of Homeland Security with NISAC was an appropriation of \$7,500,000 for the construction and equipping of a NISAC facility at Kirtland Air Force Base in Albuquerque, New Mexico, which is adjacent to Sandia National Lab. Those funds have not been released for their intended purpose.

Question. What is the delay in moving forward on this important facility?

Answer. IAIP continues to move forward with the plans to build the facility, giving full consideration to the elements of the program and our obligation to comply with NEPA and other Federal statutes applicable to Federal construction projects.

Question. What is the status of the \$7,500,000 appropriation specifically for the NISAC facility? Are those funds being held for the intended purpose?

Answer. IAIP continues to move forward with the plans to build the facility, giving full consideration to the elements of the program and our obligation to comply with NEPA and other Federal statutes applicable to Federal construction projects.

Question. When can the Subcommittee expect the Department of Homeland Security to break ground on the NISAC facility in New Mexico?

Answer. IAIP continues to move forward with the plans to build the facility, giving full consideration to the elements of the program and our obligation to comply with NEPA and other Federal statutes applicable to Federal construction projects.

QUESTION SUBMITTED BY SENATOR LARRY CRAIG

Question. Gen. Libutti I would like to compliment you on your approach to working with the national laboratories. It is clear that your management team is committed to using the best capabilities available in the most efficient way. In that vein, I would like to invite you to visit the Idaho National Engineering and Environmental Laboratory to learn more about how INEEL can contribute to your engineering, testing, and evaluation needs. The INEEL is in the process of standing up its national Critical Infrastructure Protection Test Range. Your organization is now using some of the resources that exist there. I think you will find it valuable to learn first hand the breadth of capabilities they have to offer your organization and their abilities to help you accelerate the implementation of many of your programs.

In the longer term, I presume that testing and evaluating technologies before deployment by IAIP will be an important part of your mission.

How much value do you see in having a national critical infrastructure protection test range available to you to accomplish your mission?

Answer. I see great value in a facility that gives DHS the ability to test and evaluate infrastructure protection Technologies. As you noted, the Idaho National Engineering and Environmental Laboratory (INEEL) provides just such a Test and Evaluation (T&E) and modeling capability to DHS to help guide the development of critical infrastructure protection systems.

INEEL has functional electrical grids, nuclear power plants and chemical processing facilities on its premises. INEEL engineers have been using this facility to conduct vulnerability and risk assessments on critical infrastructure for years. Furthermore, the test range itself is located in a remote and isolated area, giving the INEEL staff the freedom to conduct real world, hands-on vulnerability assessments without placing a local population at risk.

As you may know, the Protective Security Division (PSD) of IAIP already is working with INEEL to address the vulnerabilities of our Nation's critical infrastructure by developing a National SCADA Testbed and a Process Control Security and Vulnerability Reduction Center. This new and important partnership between DHS and INEEL will help protect the Nation's critical infrastructure systems from both inadvertent failures and malicious attacks.

QUESTIONS SUBMITTED BY SENATOR ROBERT C. BYRD

CRITICAL INFRASTRUCTURE PROTECTION

Question. The budget for remediation and protection of critical infrastructure includes the identification of critical infrastructure and assessing vulnerabilities in addition to implementing remediation and protection measures. For fiscal years 2004 and 2005, please estimate, by critical infrastructure sector, the amounts actually spent or planned to be spent on identifying critical infrastructure and assessing vulnerabilities versus the amount spent on remediation or protection of critical infrastructure. For protective measures, please distinguish between investments made for "buffer zones" versus investments made to harden security "on site."

According to the Department, 85 percent of the critical infrastructure is owned by the private sector. In assessing the need for Federal investments to secure our critical infrastructure, it will be essential for Congress to have measurable benchmarks of private sector investments in such infrastructure, such as investments in chemical facilities, port security, and cyber-security. Please provide the subcommittee with any benchmarks that have been established that show the private sector is making the necessary investments to secure our critical infrastructure and key assets.

Please explain in detail how the \$19,900,000 appropriated in fiscal year 2004 and the \$19,900,000 requested in fiscal year 2005 will be spent for "Protective Security Centers." How many centers have been established or planned to date and where are they located? How much funding is needed for each center? What purpose does each center serve?

Answer. As a result of a mid-year review, two Protective Security Centers are planned for fiscal year 2004; one is linked to NYPD and another to LAPD. These centers, at a total cost of \$10 million, will assist DHS to (a) identify critical assets in metropolitan areas for inclusion in national databases; (b) create partnerships between the police departments and protective security officials in the private sector to focus on combined protective activities; (c) reinforce Federal-State-local incident management procedures; and (d) develop training and exercise programs focused on protection vice response. Additional centers may be established in fiscal year 2005 and strategically located across the country to best serve law enforcement agencies. Funds are being used for the physical build-out and furnishing of the Centers with required infrastructure, computers and other necessary equipment and supplies. The respective police departments will staff the Centers.

CHEMICAL PLANT SECURITY

Question. The General Accounting Office recently testified that "despite the industry's voluntary efforts, the extent of security preparedness at U.S. chemical facilities is unknown."

Explain IAIP's role in assessing vulnerabilities and taking protective at chemical security plants? How much of IAIP's fiscal year 2004 and fiscal year 2005 budget, respectively, is dedicated to chemical plant security. For each fiscal year, please specify the amount spent or planned for vulnerability assessments, the number of chemical plants IAIP will provide vulnerability assessments for in fiscal years 2004 and 2005, and provide the amount planned for protective actions. Please specify, in detail, the protective actions IAIP will take in fiscal years 2004 and 2005 to secure chemical plants. Provide the amount of funding that is being spent to secure the area surrounding chemical plants versus funding being spent to harden security at the chemical plants themselves.

Due to the dynamic threat environment combined with the ongoing effort to identify and prioritize the Nation's critical infrastructure and key assets (CI/KA), IAIP budgets reflect efforts to reduce vulnerabilities across all sectors to maximize flexibility in responding to emerging threats. That said, in fiscal year 2004 over \$38.5 million of PSD's budget was dedicated to collecting, cataloging, and analyzing vulnerability assessment information across all sectors. The President's fiscal year 2005 budget has dedicated \$38.7 million towards these efforts, enabling us to continue to reduce the vulnerabilities of our Nation's CI/KA.

DHS has conducted approximately 19 Site Assistance Visits (SAVs) specifically to chemical facilities to assess their common vulnerabilities. The data collected during these site-specific visits is used to produce tools to help critical infrastructure owners and operators bolster protective measures.

One such tool is the Characteristics and Common Vulnerabilities (CCVs) report series on vulnerabilities for classes of critical infrastructure and key assets (CI/KA). A CCV report for chemical facilities and a separate CCV for chemical storage facili-

ties have been produced by PSD, and both are available to owners and operators of these facilities.

Answer. We also are assisting State and local authorities, as well as private industry, in developing Buffer Zone Protection Plans (BZPPs) for areas immediately adjacent to the "fence line" of critical infrastructure. The approximately 1,700 BZPPs completed by the end of 2004, included roughly 360 chemical sites warranting special attention. For fiscal year 2004 we allocated up to \$50,000 per CI/KA site for vulnerability reduction. A data call is currently underway to support the identification of sites for attention in fiscal year 2005 and Protective Security Division (PSD) is expecting to complete roughly 2,000 BZPPs next year.

Building upon a program initiated in fiscal year 2004 (funded at \$3.25 million), the DHS fiscal year 2005 budget request has approximately \$10.8 million dedicated to the acquisition of web cam monitors for the chemical sector. These monitors will be installed adjacent to designated critical chemical sites to extend their buffer zones and enhance protective measures. DHS' plan is to provide this equipment to local law enforcement agencies to install on public right of ways to monitor the security of these facilities.

DHS also has established a protection, training, and planning program for State homeland security personnel, local law enforcement, chemical facility operators and site security personnel. Periodic drills among the protective community will be conducted to exercise chemical facilities' response plans in case of a terrorist attack. PSD will continue to work with the Office for Domestic Preparedness to incorporate chemical plant security into national exercises.

We are also in the process of developing plans for and deploying Protective Security Advisors (PSAs). Each PSA will have responsibility for a specific region of the county and will maintain a close relationship with the chemical plant owners and operations in their specific area of responsibility. PSAs will facilitate information sharing, organize protective security training, assist in emergency coordination, and represent DHS in the communities in which they are posted. Security Augmentation Teams (SATs) are also being developed. SATs will consist of about 25 personnel who are drawn primarily from major urban SWAT units. These SATs will focus on protecting high-value sites, including critical chemical facilities, will develop working relationships with the site's permanent protective security team, and will become familiar with the site's specific vulnerabilities. The PSA and SAT programs, still in their early stages and are being actively pursued.

The activities described above in fiscal year 2004 and continued in fiscal year 2005 will not only greatly increase chemical site security and across all other sectors, but will increase our Nation's general protective capacity.

INTEGRATED TERRORIST WATCH LIST

Question. What resources, if any, are being used in fiscal year 2004 and planned for fiscal year 2005 to integrate lists of terror suspects held by different agencies? What is the timeline for having a fully functional integrated watch list? What role will IAIP play in the Terrorist Screening Center?

Answer. The Department of Homeland Security is allocating approximately \$8,000,000 to the Terrorist Screening Center (TSC) for fiscal year 2004. In fiscal year 2005, DHS will not contribute funds to the TSC, but will provide personnel detailed from DHS to the center. Information Analysis and Infrastructure Protection (IAIP) Directorate personnel will continue DHS' contribution to this effort by maintaining ongoing communication and coordination with the center. The Terrorist Screening Center (TSC) is fully operational now. On December 1, 2003 the TSC began 24/7 call center operations, coordination of the U.S. Government response, ensuring information collected was distributed to the appropriate entities, and established a process for addressing outdated and erroneous terrorist records and misidentifications. The database, TSDB, is currently limited to use at the TSC and will undergo several enhancements between now and the end of the (calendar) year. At that time, agencies will be able to electronically query the TSDB directly and get a systematic response within seconds. Because the TSC now maintains the terrorist information in the multiple systems used, it can ensure all the information appropriate for these systems is included.

IAIP STAFFING

Question. According to information the IAIP directorate provided to the subcommittee, only 263 of 729 authorized positions were on board at the end of February, 2004. IAIP projects that only 543 positions will be filled by the end of fiscal year 2004. It would appear that IAIP will be lapsing millions of dollars that Congress approved for staffing. Do you intend to send the Committee a plan for reallo-

cating these funds? If so, provide a detailed plan for spending these excess funds in fiscal year 2004.

Answer. A memorandum requesting reprogramming/transfer actions has been submitted to congressional committees. This request notifies the committees that IAIP will redirect \$23,500,000 from salaries object classes to other object classes for securing space to meet IAIP requirements.

OBLIGATED FUNDING

Question. On March 1, the IAIP directorate provided the subcommittee with an estimate of \$426,077,292, which represented the amount of fiscal year 2004 appropriated funds that either have been obligated or committed. Please provide the amount obligated versus committed. In addition, provide the amount of funding planned to be spent via contract in fiscal years 2004 and 2005 versus in-house.

Answer. As of March 1 (February 29 accounting report), IAIP obligations were \$199,255,217. The remainder of \$226,822,073 was commitments on March 1 that are not yet signed contracts. As an update to this answer, IAIP obligations as of March 31 were \$364,419,840, and as of April 30 were \$382,475,764.

All of the IAIP Assessment and Evaluation funding of \$711,085,630 will be spent via contract or intergovernmental payment. In house salaries and expenses are in a separate Salaries and Expenses appropriation.

SUBCOMMITTEE RECESS

Senator COCHRAN. Let me thank both of you for your cooperation with our subcommittee and your attendance at the hearing this morning. We hope that we will continue to be able to work closely with you as we work our way through the budget process, and that we provide the funds you need to do your job and carry out your mission successfully.

I don't think we have any more important responsibility in government than what we're doing here in the Department of Homeland Security and in this subcommittee that provides the funding for these activities.

We will stand in recess until the next hearing of our subcommittee when we will continue our review of the 2005 budget request. We will have a hearing on March 9, in this same room. Our witness at that time will be the Under Secretary for Border and Transportation Security, the Honorable Asa Hutchinson.

Until then we stand in recess.

[Whereupon, at 11:47 a.m., Tuesday, March 2, the subcommittee was recessed, to reconvene at 10 a.m., Tuesday, March 9.]