HOMELAND SECURITY SCIENCE AND TECHNOLOGY BUDGET HEARING FOR FISCAL YEAR 2005

HEARING

OF THE

SUBCOMMITTEE ON CYBERSECURITY, SCIENCE, AND RESEARCH AND DEVELOPMENT

BEFORE THE

SELECT COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

FEBRUARY 25, 2004

Serial No. 108–37

Printed for the use of the Select Committee on Homeland Security

Available via the World Wide Web: http://www.access.gpo.gov/congress/house

U.S. GOVERNMENT PRINTING OFFICE

22–453 PDF WASHINGTON : 2005

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

SELECT COMMITTEE ON HOMELAND SECURITY

CHRISTOPHER COX, California, *Chairman*

JENNIFER DUNN, Washington
C.W. BILL YOUNG, Florida
DON YOUNG, Alaska
F. JAMES SENSENBRENNER, JR., Wisconsin
W.J. (BILLY) TAUZIN, Louisiana
DAVID DREIER, California
DUNCAN HUNTER, California
HAROLD ROGERS, Kentucky
SHERWOOD BOEHLERT, New York
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania
CHRISTOPHER SHAYS, Connecticut
PORTER J. GOSS, Florida
DAVE CAMP, Michigan
LINCOLN DIAZ–BALART, Florida
BOB GOODLATTE, Virginia
ERNEST J. ISTOOK, JR., Oklahoma
PETER T. KING, New York
JOHN LINDER, Georgia
JOHN B. SHADEGG, Arizona
MARK E. SOUDER, Indiana
MAC THORNBERRY, Texas
JIM GIBBONS, Nevada
KAY GRANGER, Texas
PETE SESSIONS, Texas
JOHN E. SWEENEY, New York

JIM TURNER, Texas, *Ranking Member*
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
BARNEY FRANK, Massachusetts
JANE HARMAN, California
BENJAMIN L. CARDIN, Maryland
LOUISE MCINTOSH SLAUGHTER, New York
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ROBERT E. ANDREWS, New Jersey
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
KAREN MCCARTHY, Missouri
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., North Carolina
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
KEN LUCAS, Kentucky
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida

JOHN GANNON, *Chief of Staff*
STEPHEN DEVINE, *Deputy Staff Director and General Counsel*
THOMAS DILENGE, *Chief Counsel and Policy Director*
DAVID H. SCHANZER, *Democrat Staff Director*
MARK T. MAGEE, Democrat *Deputy Staff Director*
MICHAEL S. TWINCHEK, *Chief Clerk*

SUBCOMMITTEE ON CYBERSECURITY, SCIENCE, AND RESEARCH AND DEVELOPMENT

MAC THORNBERRY, Texas, *Chairman*

PETE SESSIONS, Texas, *Vice Chairman*
SHERWOOD BOEHLERT, New York
LAMAR SMITH, Texas
CURT WELDON, Pennsylvania
DAVE CAMP, Michigan
ROBERT W. GOODLATTE, Virginia
PETER KING, New York
JOHN LINDER, Georgia
MARK SOUDER, Indiana
JIM GIBBONS, Nevada
KAY GRANGER, Texas
CHRISTOPHER COX, California, *Ex Officio*

ZOE LOFGREN, California, *Ranking Member*
LORETTA SANCHEZ, California
ROBERT E. ANDREWS, New Jersey
SHEILA JACKSON-LEE, Texas
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
CHARLES GONZALEZ, Texas
KEN LUCAS, Kentucky
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida
JIM TURNER, TEXAS, *Ex Officio*

CONTENTS

Page

STATEMENTS

The Honorable Mac Thornberry, a Representative in Congress From the State of Texas, and Chairman, Subcommittee on Cybersecurity, Science, and Research and Development 1
The Honorable Zoe Lofgren, a Representative in Congress From the State of California, and Ranking Member, Subcommittee on Cybersecurity, Science, and Research and Development
Oral Statement 3
Prepared Statement 2
The Honorable Christopher Cox, a Representative in Congress From the State of California, and Chairman, Select Committee on Homeland Security 39
The Honorable Jim Turner, a Representative in Congress From the State of Texas, Ranking Member, Select Committee on Homeland Security
Oral Statement 40
Prepared Statement 4
The Honorable Robert E. Andrews, a Representative in Congress From the State of New Jersey 36
The Honorable Bob Etheridge, a Representative in Congress From the State of North Carolina 43
The Honorable Kay Granger, a Representative in Congress From the State of Texas 45
The Honorable Pete Sessions, a Representative in Congress From the State of Texas 46

WITNESS

Dr. Charles E. McQueary, Under Secretary for Science and Technology, Department of Homeland Security
Oral Statement 5
Prepared Statement 8

APPENDIX

MATERIAL SUBMITTED FOR THE RECORD

Questions for the Record From The Honorable Mac Thornberry 61
Questions for the Record From The Honorable Jim Turner 63
Questions for the Record From The Honorable Kendrick B. Meek 67

HOMELAND SECURITY SCIENCE AND TECHNOLOGY BUDGET HEARING FOR FISCAL YEAR 2005

Wednesday, February 25, 2004

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CYBERSECURITY, SCIENCE,
AND RESEARCH AND DEVELOPMENT,
SELECT COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The Subcommittee met, pursuant to call, at 1:04 p.m., in Room 2325 of the Rayburn House Office Building, Hon. Mac Thornberry [Chairman of the Subcommittee] presiding.

Present: Representatives: Sessions, Camp, Granger, Cox, Lofgren, Andrews, Christensen, Etheridge, Lucas, Langevin, Meek, and Turner.

Mr. THORNBERRY. The Subcommittee will come to order. I want to welcome the members, the witness, to our hearing today, which is going to focus on the Department of Homeland Security's budget for science and technology. Next Monday, the Department will mark its one year birthday. It seems to me this is an appropriate time to measure how much progress has been made over the past year, and assess where we are now, and also plan on where we—how we move ahead. And I am also cognizant of the fact that as September 11 recedes further back into our memory, it is a challenge to maintain the sense of urgency, both in improving operations of the Department and also in the day to day job of making our country safer.

I personally believe that there are five areas in which the Department and Congress ought to focus in our second year efforts. One is integrating the Department into that one seamless unit that we intended it to be. Two is improving coordination with the private sector, with other government entities, and ultimately, also international entities. Three is improving intelligence analysis and sharing. Four is developing ways to measure whether we are really making the country safer. And five is developing and fielding technology, which of course, is the subject of our hearing today.

Most of us acknowledge that central to success in the war on terrorism is fielding of technologies that can help prevent attack, as well as those that help us to respond quickly and effectively when something does occur; but deciding what to buy, and in which technology—technologies to invest involves setting priorities, and to a certain extent, in making educated guesses. It also involves not

buying everything that somebody has for sale, and having the discipline to invest for longer term solutions.

The first step was to get the building blocks in place, the people, the organizations, the processes to make decisions; and my view is that the S & T Directorate has done a good job so far in setting those cornerstones. The next step is to begin making decisions, whether it is identifying an existing technology that you want to field quickly, or developing a technology to a more useful application, or directing research dollars into some area where you have vulnerabilities.

For Fiscal Year 2005, the Administration has requested just a little over a billion dollars for the S & T Directorate, about $126 million more than last year. The largest increase over last year is for biosurveillance. Other parts of the Department of Homeland Security, as well as other Cabinet agencies, also have Homeland Security-related science and technology funding, and one of the issues we will want to explore is how that is coordinated. The bottom line, it seems to me, is that we are safer than we were a year ago, but we are not nearly as safe as we should be, or as safe as we will be. Technology, in our ports, in our cities, or in our squad cars, are going to help us all do a better job of protecting Americans.

With that, I will yield to the distinguished Ranking Member, the gentlelady from California, for any statements she would like to make.

Mr. LOFGREN. Thank you, Mr. Chairman, and I ask unanimous consent to put my entire statement into the record.

Mr. THORNBERRY. Without objection.

[Statement of Ms. Lofgren follows:]

PREPARED OPENING STATEMENT OF THE HONORABLE ZOE LOFGREN, RANKING MEMBER SUBCOMMITTEE ON CYBERSECURITY, SCIENCE, AND RESEARCH AND DEVELOPMENT

Today is the first hearing of the Homeland Security Subcommittee on Cybersecurity, Science and Research and Development in 2004. This subcommittee accomplished much in the past year since its initial creation, and let me once again state how much I have enjoyed working with our chairman, Congressman Mac Thornberry and his staff. I look forward to working with you, and have high expectations for the coming year.

Today we will hear from Under Secretary Charles E. McQueary of the Department of Homeland Security's Science and Technology Directorate. Dr. McQueary was the first person to testify before this subcommittee last year, and I want to thank you for appearing before us once again today.

At the time of last year's hearing, Dr. McQueary was new to the job, and he spoke about his priorities for the S & T Directorate, and mentioned 7 specific areas of emphasis for the Directorate. These included the following:

1. Develop and deploy state-of-the art, high-performance, low operating-cost systems to prevent the illicit traffic of radiological/nuclear materials and weapons into and within the United States.
2. Provide state-of-the art, high-performance, low operating-cost systems to rapidly detect and mitigate the consequences of the release of biological and chemical agents.
3. Provide state-of-the art, high-performance, low operating-cost systems to detect and prevent illicit high explosives transit into and within the United States
4. Enhance missions of all Department operational units through targeted research, development, test and evaluation (RDT & E), and systems engineering and development.
5. Develop and provide capabilities for protecting cyber and other critical infrastructures.
6. Develop capabilities to prevent new-technology as a surprise weapon by anticipating emerging threats.

7. Develop, coordinate and implement technical standards for chemical, biological, radiological, arid nuclear (CBRN) non-medical countermeasures.

Dr. McQueary proposed an ambitious agenda at that first hearing and the Members of this subcommittee were willing to give the Directorate some time to organize.

Dr. McQueary, you have been on the job at DHS for almost a year. Now is an appropriate time for this subcommittee to get a report from you on your progress. We want to learn about the status of your stated priorities, and if they have changed as a result of your experiences over the past year.

We also will spend a considerable amount of time today looking at your fiscal year 2005 budget request. This year's request is $1.04 billion, which is an increase over last year's enacted budget of $912.9 million. As you know, this budget proposal invests heavily in biological countermeasures (over a 40 percent increase over last year's enacted budget). I want to hear how you came to decide that bio-defense is the most important priority at this time. What about chemical, nuclear, and high explosives countermeasures? Their budgets remained almost flat over last year's enacted budget. Without releasing any classified information, I hope you will take some time today to walk us through your process for assessing threats, setting priorities and investing resources.

Finally, at last year's hearing, you were questioned extensively about the process that the department uses for reviewing ideas and products from the private sector and individuals. As I am sure you recall, several members asked you about this, including Congressman Thornberry, Camp, Lucas, Congresswoman Dunn and myself. You told this subcommittee that you personally reviewed each incoming proposal and product that is sent to the directorate. Specifically, you said the following. . . .

> "The first formal thing that we put in place was the e-mail address because it was clear that we had a pent up emotional demand from people that wanted to be able to tell us about things that they're doing. . . .And what we do with those [*incoming e-mail proposals*], I actually read every one of them myself. I mean, and when I say read them, those that are many pages long, I only read the executive summary to get a sense of what's there."[1]

The fact that you reviewed each and every proposal was a bit shocking to me. I can only imagine how many incoming requests arrive at the directorate and I suspect that if you are still reviewing each one, you have very little time for anything else.

I continue to hear from people, both here in Washington and back in Silicon Valley, who have ideas and products that they would like to share with the Department. They are frustrated because they do not know where to go or who to talk within DHS. I share their frustrations. It is a major concern to me that I can't give them advice on how best to approach the staff at DHS. Some individuals have excellent and innovative ideas that merit consideration by DHS. Others may not have the best ideas, but I am not in a position to judge their thoughts on the merits. You are.

Earlier this week at a ceremony marking the first anniversary of the creation of the Department of Homeland Security, Secretary Tom Ridge outlined several goals for DHS in 2004. One of these goals was the creation of a "Private Sector One-Stop Shop." He described this shop as a "robust web and personal assistance service venue where all elements of the business community can learn how to do business with the department."

I have many questions about this shop that I hope you will answer today. How will this one-stop shop work? Where in the Department will it be located? What is the difference between this and the "technology clearinghouse" provided for in the Homeland Security Act, Sec. 313? Is this just a way to send information to the department, or will it also include an ability to interact directly with DHS officials? I hope you are not still in the business of reviewing each incoming e-mail and that this one-stop shop will be effective. I look forward to learning more about it today.

Before I conclude, I want to thank the Democratic staff on the Homeland Security Committee for their hard work. In particular, David Grannis was particularly helpful in preparing for today' shearing.

Ms. LOFGREN. First, this is our first hearing of the—of this year, and I think when we look back over the last year, we did accomplish a lot, but there is much, much more to do, as you have just referenced, and thinking back to when we first met with Dr.

[1] I Undersecretary of Homeland Security Charles McQueary in testimony before the House Subcommittee on Cybersecurity, Science, and Research and Development; May 21, 2003.

McQueary last year, he spoke about seven specific areas that he wished to focus in on.

I am hoping today to get an update on all seven of those, and where we stand with each of them. As you have mentioned, in the budget, there is a strong emphasis on biodefense. I am interested in how, to the extent you can discuss that in an unclassified setting, we reached the conclusion that that was our highest priority, as compared to other threats, chemical, nuclear, high explosives, and the like.

The other thing I hope you can touch on, and I have mentioned it to the Chairman, we may want to propose having some further discussions, in—either in a workshop format or the like, is to pursue further the interface between the private sector and your shop.

I still hear concerns that people don't know who to talk to, how to be heard. Clearly, I remember last time we met, you mentioned, and it actually made me—it scared me here, that you were reading all the emails. I am sure that that can no longer be the case.

Mr. MCQUEARY. That is correct.

Ms. LOFGREN. And that is good news. But I want to know about the processes in place, and I—without being unduly negative, note that we need to do a better job here, because I—the members of the Committee are constantly being approached with—by private sector people with suggestions. We shouldn't really be the entry point for the Department. We are not skilled to do that, and so I am hopeful that we can come up with—I mean there are so many great ideas out there, but some of them are also vaporware, and so somebody needs to sort through what is real, what isn't, what can be applied, and in a way that is better than what we are doing now.

So, I am hopeful to hear about the private sector one stop shop, where that is, and where it is going to be located, and how we can deploy it. And with that, I would just like to mention, again, what a pleasure it has been to work with the Chairman, Mr. Thornberry, and I look forward to another good year.

Mr. THORNBERRY. I thank the gentlelady, and it is also my pleasure in working with her. All members may, without objection, have opening statements submitted for the record, unless there is a member who would like to make an oral opening statement, we will turn to our witness at this point.

PREPARED STATEMENT OF THE HONORABLE JIM TURNER, RANKING MEMBER, SELECT COMMITTEE ON HOMELAND SECURITY

Thank you Mr. Chairman.

Under Secretary McQueary, welcome back. We appreciate your testimony today.

As you may know, the Democratic Members of this Committee issued a report today entitled "America at Risk: Closing the Security Gap." A principle reason why we issued the report was to underscore that while the nation is more secure one year after the creation of the Department, it is not as secure as it needs to be. Additional measures, supported by appropriate resources, need to be taken to ensure the safety and security of our homeland. I hope that the Department will take a close look at the report and that we can work together to implement its recommendations.

Closing our existing security gaps will require the continued efforts of the Department's Science and Technology Directorate. I appreciate you being here to give us a better understanding of how the budget request for the Science and Technology Directorate for Fiscal Year 2005 will do this. The hearing will help us produce the first ever Department of Homeland Security authorization bill.

Let me first say that this Directorate, under your leadership, has made great strides to build an institution from scratch. And my staff informs me that your staff has been very accessible and helpful throughout the past year.

My two largest concerns today are whether the top line of your Directorate's budget request is sufficient, given the importance of your research and development work, and whether it will be spent in the most effective way to improve homeland security.

The President's Fiscal Year 2005 budget request for the Directorate is about $1 billion, representing a $127 million, or 14 percent, increase above the current year levels. Outside of the portfolio for biological research and development, the request is almost exactly the same as what Congress appropriated for the current year.

I think it's important, however, to put the budget into greater context. The DHS budget is only about one third of the Administration's total request for homeland security research and development of $3.6 billion. It is less than two percent of what was requested for the Department of Defense for research and development, and less than one percent of the total President's total R & D budget.

In this context, I am concerned that we may not be devoting sufficient resources to the science and technology programs within the Department of Homeland Security. We could be moving faster and stronger to protect the homeland.

For example, I mentioned that the Fiscal Year 2005 budget request for radiological and nuclear countermeasures and for the chemical countermeasures are flat. Even the Department's own strategic plan released earlier this week underscores the need for better technologies to detect nuclear, biological, and chemical weapons.

There are Customs and Border Protection officials at the nation's ports of entry that don't have the ability to detect nuclear materials in containers and cargo. Our nation's first responders are frequently called to investigate suspicious white powders, and are unable to tell whether it is ricin, anthrax, or powdered donut. So I am concerned that these research and development portfolios are not commensurate with the security gaps that exist.

Secondly, I have concerns with the way funds are prioritized within the Directorate's budget request. During a hearing of this Subcommittee's late last fall, we heard about the Directorate's process for allocating funds across research and development portfolios by speculating on the sophistication and potential damage caused by different terrorist attacks. But that process does not include intelligence on the likelihood that terrorists will attempt a given type of attack or information on what capabilities a terrorist group has to carry out an attack.

Your Directorate should be getting this information as part of a comprehensive threat and vulnerability assessment from the IAIP Directorate. While this responsibility clearly falls outside of your Directorate, I expect that future budget decisions will be made on the basis of this information.

The Directorate has also decided to prioritize short-term development at the expense of longer-term research. While the urge to deploy important and nearly-mature products out into the field is understandable, I believe the Directorate will need to begin shifting additional resources towards developing the next-generation of homeland security technologies.

Mr. Under Secretary, the Science and Technology Directorate has made impressive strides since it was created in the Homeland Security Act, and I commend you for your leadership. I urge you to work with your colleagues to ensure that threats and vulnerabilities are fully assessed when preparing your budget. And I hope this Committee can work with you to ensure that you have all the resources that are necessary to advance your important homeland security work.

Let me welcome back before the Subcommittee Dr. Charles E. McQueary, Under Secretary for Science and Technology of the Department of Homeland Security. And you are recognized, sir.

STATEMENT OF CHARLES McQUEARY, UNDER SECRETARY SCIENCE AND TECHNOLOGY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. MCQUEARY. Thank you very much. I would like to say good afternoon to you, Chairman Thornberry, Congresswoman Lofgren, and the distinguished members of the panel, my good friend from North Carolina, Congressman Etheridge. It is a pleasure to be here 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 support the efforts of the dedicated men and women who protect and secure our homeland.

When I first reported to you about our activities last May, we had just begun our work. The Directorate has accomplished much since its inception last March 1, and I would like to give you some of those highlights.

We have deployed monitoring systems that operate continuously to detect biological pathogens in approximately 30 U.S. cities.

We have also set up test beds to provide accurate radiation and nuclear warnings at air and marine cargo 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 us put needed technologies into the hands of responders quickly.

And the Homeland Security Advanced Research Project Agency has started extensive research for next generation biological and chemical and 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.

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 interagency working groups.

In accomplishing this, we have doubled the staff of this Directorate with some of the country's brightest and most dedicated people. We started this Directorate with 87 people, 53 of whom were transferred in from the Environmental Measurements Laboratory in New York, and so we had a very small staff to start. Today, we are at about 212 people.

However, 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.

The Science and Technology Directorate has prioritized its research and development efforts based upon the directives and recommendations from many sources, and I will only mention a few of those here, although the complete list is in my written testimony: the Homeland Security Act of 2002, President Bush's National Strategies and 9 Homeland Security Presidential Directives, the report from the National Academies of Sciences on "Making the Nation Safer," and reports from the Gilmore, Bremer, and Hart-Rudman Committees.

We have identified and integrated into the information in these sources for review and evaluation by our scientific staff, and it

provides the basis for determining the R & D needed to meet our mission. We recognize that many organizations are contributing to the homeland security science and technology base.

In the Homeland Security Act of 2002, Congress recognized this as well, and 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, and I can assure you we take this responsibility very seriously.

We began this coordination process by evaluating and producing a report on Department of Homeland Security R & D activities underway that were not under the direct cognizance of the Science and Technology Directorate, and, where appropriate, S & T will absorb these R & D functions. We are now initiating the effort needed to coordinate homeland security research and development across the entire United States Government, and that is a large challenge, as you obviously would know. Discussions are ongoing with 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.

In the area of the budget request, what I would like to do is very briefly describe our Fiscal Year 2005 plans. We have an overall budget request of $1.04 billion, which is an increase of $126.5 million, or almost 14 percent over the Fiscal Year 2004 levels. With these funds, Science and Technology will continue to make progress in securing the homeland.

For example, under President Bush's new biosurveillance 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 cybersecurity, both through partnerships and by creating low-cost, high-impact solutions to identified cybersecurity challenges. We will ramp up our work in counter MANPADS (man-portable air defense systems), to improve technologies to protect the commercial aircraft from this threat. We will award contracts in fiscal year 2005 for integrating commercial prototype equipment on selected commercial aircraft, and conduct tests and evaluate—and conducting tests and evaluation, including live fire range tests.

In less than a year, the science and the engineers of the Science and Technology Directorate have accomplished more than I could have expected. I am proud to have shared with—some of these success stories with you here today. We have appended a more comprehensive summary of accomplishments to date for the record. As yet, we also recognize—and yet, we also recognize there is much to do, which is the point you have made, and I fully agree, and we will be working just as hard in 2005 to make further progress.

I look forward to working with you and my colleagues in other Federal agencies and with private industry and academia to

continue this work and improve our ability to protect our homeland. This concludes my prepared statement, and I would welcome the opportunity to take questions, if I may, at this time.

[The statement of Mr. McQueary follows:]

PREPARED STATEMENT OF DR. CHARLES E. MCQUEARY UNDER SECRETARY FOR SCIENCE AND TECHNOLOGY, DEPARTMENT OF HOMELAND SECURITY

Introduction

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

The Nation's advantage in science and technology is key to securing the homeland. The most important mission for the Science and Technology Directorate is to develop and deploy cutting-edge technologies and new capabilities so that the dedicated men and women who serve to protect and secure our homeland can perform their jobs more effectively and efficiently—these men and women are my customers.. When I last reported to you about our activities, we had just started our work. Since its inception less than a year ago, the Science and Technology Directorate has:

(1) deployed continuously operating biological pathogen detection systems to approximately 30 United States cities;

(2) set up testbeds for radiation and nuclear warnings at air and marine cargo ports in cooperation with the Port Authority of New York and New Jersey,

(3) established the first series of interoperability guidelines for the Nation's wireless emergency communications network;

(4) established the first national standards guidelines for radiation detection equipment;

(5) awarded the first Homeland Security Fellowships and Scholarships;

(6) established the first Homeland Security University Center of Excellence,

(7) transferred the Plum Island Animal Disease Center from the Department of Agriculture to the Science and Technology Directorate;

(8) 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;

(9) 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;

(10) 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.

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

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 dollars to enhance and expand the BioWatch Program.

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

Biological Countermeasures

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

In 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 Bio Watch, 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 (three-year), and long-term (five-plus year) capabilities. We will qualify candidate off-the-shelf sensors for demonstration in an application to facilities protection. We will also address response and recovery. Working with the user community, we will develop first-generation playbooks for responding to the three reference scenarios and develop technical requirements for personal protection equipment.

High Explosives Countermeasures

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

This portfolio in 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, three-year research project to create an experimental infrastructure network to support development and demonstration of next-generation information security technologies for cyber defense. This is a multi-university project led by the University of California at Berkeley.
- Developed a Decision Support System focused on prioritizing investment, protection, mitigation, response, and recovery strategies related to Critical Infrastructure Protection. The initial proof-of-concept began in August 2003 and a case study is being conducted in February 2004. The prototype model will include representation of all 14 critical infrastructure sectors/assets and their interdependencies.
- Developed advanced algorithms for speeding the creation of DNA signatures for biological pathogen detection through the Advanced Scientific Computing Research and Development program. These discoveries will result in cheaper, faster and more reliable bio-detectors for homeland security.

In 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 Departments 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 highvisibility venues.

Support to Border and Transportation Security

The Science and Technology Directorate supports all elements of BTS enforcement and facilitation processes through identifying operational requirements, developing mission capabilities-based technological needs and implementing a strategic plan. We are providing systems engineering support to various BTS programs including US–VISIT and Unmanned Aerial Vehicles.The Science and Technology Directorate's support to the BTS Directorate is accomplished by implementing a capabilities-based technology planning process. The capabilities-based approach establishes the scope of effort and framework for a technology plan. Through a series of user conferences and technology opportunity conferences, requirements are developed and prioritized for new and improved capabilities. Operational personnel identify capabilities and technology personnel identify potential development opportunities. Capability gaps and possible technology solutions are proposed, and a budget is developed to distinguish between both funded and unfunded needs.

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

In 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 HAWKEYE program injects technologies (such as Surveillance, Command & Control, Sensor Fusion, and Communications) allowing simultaneous evaluation of technology performance as a direct impact on mission execution.

Support to the United States Secret Service

We have coordinated with the United States Secret Service and established its first direct-funded R & D program. Based upon appropriated funding, four initiatives have been identified and prioritized, and are underway in 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 three-year contract whose annual cost we account for in our planning.

Counter-MANPADS

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

Over the past year, we have had a successful solicitation announcing a program to address the potential threat of MANPADS to commercial aircraft. White papers responding to the Counter-MANPADS program solicitation were reviewed by technical experts from the Department of Homeland Security, Department of Defense, and other government agencies; proposals were evaluated; and awards were made to three contractor teams to perform the first of two program phases, which began in January, 2004. The first phase will result in a preliminary design and a test plan to demonstrate missile countermeasure equipment on selected commercial aircraft.

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

SAFECOM

The SAFECOM (Wireless Public SAFEty Interoperable COMmunications) program is the umbrella initiative to coordinate 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 seven 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 informa-

tion 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 willinclude sustainable environmental monitoring capability for metropolitan areas; a national special security event system for the nation at large; and identification of needs for vaccines and therapeutics for people and animals. Longer term research will support the development of biological threat warning and characterization systems that address both current and future threats.

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

Performance Measures	FY2005 Target
Integrated field demonstrations of next-generation solutions (Domestic Demonstrations and Applications Program).	2 Demos operational
Validated human and agricultural bioassays.	10

ST0002 Chemical Countermeasures
Long term performance goal

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

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

ST0003 Chemical High Explosives
Long term performance goal

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

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

ST0004 Radiological & Nuclear Countermeasures
Long term performance goal

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

Performance Measures	FY2005 Target
Federal, state and local sites that are integrated into an operational secondary reachback architecture to resolve radiological and nuclear alarms.	5
Performance measures associated with Test and Evaluation (T and E) of developmental prototypes of Radiation Detectors. Establish a long-range plan for T and E capability.	Milestone will be achieved
Progression on planned capability development for Nuclear Incident Management and Recovery. Demonstrate 2 advanced detection technologies.	Milestone will be achieved
Progression on pre-planned product improvement of deployed technologies. Perform critical design reviews for Phase One technology improvements for projects awarded in 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	FY2005 Target
Improvement in the national capability to assess threats and vulnerabilities to terrorist attacks: 10 categories to be assessed.	Improvement in 7 categories

ST0006 Standards
Long term performance goal

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

Performance Measures	FY2005 Target
Long-term implementation of SAFETY Act FY2005 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 devicesfor federal, state, and local users will be published.	Certifications Milestones will be achieved

ST0008 Homeland Security Fellowship Programs I 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	FY2005 Target
To increase the nation's science and technology workforce and research 200 students 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 performance goal new and emerging threats, and to exploit technology development opportunities as they arise.

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

ST0010 Rapid Prototyping
Long term performance goal

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

Performance Measures	FY2005 Target
Technologies prototyped or commercialized.	3

ST0011 SAFECOM
Long term performance goal

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	FY2005 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	FY2005 Target
Effective technology/technologies for commercial aircraft to defeat manportable 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	FY2005 Target
Improved capability of DHS Components to secure the homeland as measured by assessment of customer organizations in accomplishing agreed-upon areas of assistance.	Baseline

Short-Term and Lone-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 $)

Fiscal Year	FY 2003(actual)	FY 2004(estimated)	FY 2005(proposed)
Basic	47	117	80
Applied	59	56	229
Developmental	398	608	643

Science and Technology Directorate R & D Investments (in millions of $)—Continued

Fiscal Year	FY 2003(actual)	FY 2004(estimated)	FY 2005(proposed)
Total	504	781	952
% basic	9.3%	15.0%	8.4%

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

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

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

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

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

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

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

- Dedicated and accredited bio-forensic analysis capabilities to support attribution of the use of bio-threat agents (BTA) by criminals, non-state, and state-sponsored actors
- Laboratory-based, scientific data from the analysis and assessment of biological threats to human health and agriculture to support a national bio-defense net assessment fundamental to development of national plans, risk assessment evaluations and priorities to deter, detect, mitigate and recover from BTA attack
- Applied models, materials, and validation processes to evaluate BTA countermeasures

- Evidenced-based subject matter expertise to integrate, analyze and distribute critical bio-defense and related information assembled from multiple sources through a high security and open clearinghouse.

Transfer of R & D Budgets and Activities from Other Directorates

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

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

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

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

Research and Development activities are ongoing in 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 Cybersecuritv 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 dollars.

An important component of the cybersecurity program is coordination with others who are performing cyber research and who are responsible for cybersecurity. For example, our 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 and 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, Congresswoman Lofgren and Members of the Subcommittee, this concludes my prepared statement. I thank you for the opportunity to appear before this committee and will be happy to answer any questions you may have.

Appendix

Accomplishments of the Science and Technology Directorate

Department of Homeland Security

MARCH 2003 TO FEBRUARY 2004

Biololgical and Chemical Countermeasures

Biowatch: National Urban Monitoring for Biological Pathogens

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

PROTECT (Program for Response Options and Technology Enhancement 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 Counterrorism 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 A ward 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, handheld 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 and Development program achieved an important milestone in the speed acceleration of software used to develop advanced biodetectors. Scientists have made a pair of related algorithmic advances that will speed the creation of DNA signatures for pathogen detection at considerably reduced cost. These discoveries will result in cheaper, faster, and more reliable bio-detectors for homeland security.

Threat-Vulnerability Mapper

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

Critical Infrastructure Protection Decision Support System

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

Cybersecurity

Experimental Infrastructure Network for Cyber Defense

Led by the S & T Directorate, DHS is co-funding with the National Science Foundation a $5.45M, three-year research project to create an experimental infrastructure network to support development and demonstration of next generation information security technologies for cyber defense. This project supports national-scale experimentation on emerging security research and advanced development

technologies. Called Cyber Defense Technology Experimental Research ("DETER") Network, this is a multi-university project led by the University of California, Berkley.

Evaluation Methods in Internet Security Technology

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

United States Coast Guard

Maritime Surveillance Testbed Prototype

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

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

The program has two phases; an initial prototype development phase, and an improvements and update phase. The program is expected to begin operations in June 2004 and is funded at $2.4M for fiscal year 2003 and $5M 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 one-, three-, and five-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 five-year award by early May 2004. However, current legislation states that the Institute's operation will terminate in November 2005; this issue is of concern to the bidders.

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

Homeland Security Science and Technology Advisory Committee

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

The HSSTAC was mandated by the Homeland Security Act to be a source of independent, scientific and technical planning advice for the Under Secretary for Science and Technology.

The committee will (1) advise the Undersecretary on the mission goals for the future; (2) provide advice on whether the policies, actions, management processes, and organization constructs of the Science and Technology Directorate are optimally focused on mission objectives; (3) provide advice on whether the research, development, test, evaluation, and systems engineering activities are properly resourced (capital, financial, and human) to accomplish the objectives; (4) identify outreach activities (particularly in accessing and developing, where necessary, the industrial

base of the Nation); and (5) review the technical quality and relevance of the Directorate's programs.

Countermeasures to Man-Portable Air Defense Systems

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

University and Fellowship Programs

Fellowships and Scholarships

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

University Centers of Excellence

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

Homeland Security Advanced Research Projects Agency

Near-Term Technologies

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

Detection Systems

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

Virtual Cyber Security Center

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

Small Business Innovation Research (SBIR) Program Solicitation

On November 13, 2003, the Homeland Security Advanced Research Projects Agency (HSARPA) issued a Small Business Innovation Research (SBIR) Program

Solicitation. The purpose of this solicitation was to invite small businesses to submit innovative research proposals that address eight high-priority DHS requirements:

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

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

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.

Mr. THORNBERRY. Thank you, Dr. McQueary, and let me take a second to compliment you and your folks on the full statement that you have submitted for the record.

I—you may not answer every question, but you, I think, do a very good job of going through the different areas that you all are working in, and also setting goals for 2005, and we can have this hearing again next year, and we can, as the gentlelady from California wants to ask, I know, about what you said last year, we can do it again next year, and see whether those goals have been made. And so I appreciate the work that you and your folks have done. It does help give us all confidence in what you are doing.

I am going to reserve my time at this point and yield to the gentlelady from California for any questions she might like to ask at this point.

Ms. LOFGREN. Thank you, Mr. Chairman. I just have a few questions relative to the budget, I suppose, and the first thing I want to raise has to do with the academic—university centers.

Now, I think we all thought that was a pretty good idea last year when we went through it, and—but in the budget, if I am correct, there is only $30 million allocated for this activity, and I don't think that is enough to do the centers that we—the number of centers that we talked about. I think it was appropriated $70 million, and I don't think that was all spent, so I guess that is a question. Was it all spent, and how are we going to award the 10 centers, and—that we had originally planned on, and if we are not going to do that, well, why not, and in particular, I will be a little parochial if I may, we have, in San Jose, a university center on transportation that I have heard from—not just from them, but I heard from the Navy and I also heard from Lawrence Livermore National Lab that they are doing very important work in terms of security, and—on transportation issues, and I know we have looked at ag, and we are looking at some other things, but we have infrastructure issues that are huge that I am not sure we are really dealing with in any department, and I was hoping that either with them, or—we might be able to do that. So can you address that whole issue, the university centers, for us, please?

Mr. MCQUEARY. Well, you have raised several important issues, and certainly, the request that we have in is $30 million, with $30 million for this year, or—and if one had the same amount for outgoing years, that would support approximately 3 Centers of Excellence. These are approximately $5 million, minus the—our expenses. And then, the remaining 15 will—$15 million would support another 100 Scholars and Fellows there. One of the things I have learned in this job is that we all work for someone, and it is my job—we had the adequate opportunity to debate the issue about what the size of the budget should be for the Fellows and Scholars program. At this point, I view my responsibility as one of trying to make the best performance that we can get out of the budget that has been requested, and that is what I can assure you I will do.

Ms. LOFGREN. So, without putting words in your mouth, it sounds like the 3 was a budget decision more than a policy decision that you made from your shop.

Mr. MCQUEARY. I didn't say—it is a consequence of a budget decision, yes. Okay.

Ms. LOFGREN. Okay. Was the $70 million appropriated actually spent?

Mr. MCQUEARY. No, ma'am. The—we have not spent all of the 70. In fact, without going through the rigorous details of the arithmetic, an approach that we could use, and we—I am not proposing we do this, we have enough money so that we could actually create five—a total of five centers, but the problem would be at the end of the three year period, would be—we have been allocating these for three years, there would be at least two of them that would have to be stopped, because $30 million would not be sufficient to sustain five units at that—.

Ms. LOFGREN. Well, I don't know what the Chairman thinks, but it seems to me that you can get a lot of pretty good research done in three years, especially if you are honing in to assessments, not just solutions, and as we know from the Senate hearing and the hearings we have had, we are way behind in our threat assessment activity everywhere, in cyber and in critical infrastructure, and without good assessments, you really don't have a work plan for expenditures, so I would tend to favor doing something rather than—.

Mr. MCQUEARY. Okay.

Ms. LOFGREN. I mean, that is just one person's opinion, obviously, but maybe we can get into that discussion at some point. I am also concerned about the Department of Energy labs, and I am interested in hearing about this designation of—I was surprised by intramural, extramural, what does this mean, and why was this done, and what are the implications for the various labs. I think that the feedback I have gotten from the scientific community is that those who have been designated extramural are grumpy, because they weren't good enough to be intramural. Those who have been designated intramural are grumpy, because they can't compete for funding, and nobody is happy, and so when you—so I am interested why we did this and whether we are going to continue to do this.

Mr. MCQUEARY. This has been quite a remarkable experience for me personally, to find the—what I will call the firestorm that we have been able to develop with something in which we actually thought—we truly thought and discussed this in great detail internally, and also with 9 of the labs, that we are trying to use the approach that would maximize the opportunities for the labs to participate in what we are doing, and so the logic in our thinking was as follows. Because of the charter, the—or the mission that we have, chemical, biological, radiological, and nuclear, and high explosives, some labs have more to offer in these areas than do other labs, and therefore, what we concluded is that there was a small number of the labs in which we expected to be using more than the others, and we would—and we needed to have those, we felt we needed to have those labs be participants in what I will call our internal planning and so forth, and so our conclusion was that it would not be appropriate to let those labs also compete externally, if they have insider information, so we concluded that what we should do is designate the five that we chose as the intramural labs, and with that goes the responsibility of—or the requirement that they not compete on any business or university teams for any of the work we do.

The others, what we believed we were doing was providing an opportunity for them to either compete directly for—in other areas, such as through HSARPA, where we will be spending money, or to team with private industry and/or to have a larger possibility, because had we gone down a path, quite frankly, of choosing, let us say we chose all 9 or chose all 22 and made them all intramural, meaning that we gave them full access to all of our internal information, there would be some of those labs that would get virtually no money, because they just don't have the skills and expertise that we find that we need at this time. Now, that could change later on, but at least as we look at it right now.

So we thought we were doing something that would be beneficial, but obviously, it has not been perceived that way, although one thing you did say that I have not personally encountered, those that have been designated as the intramural labs, I have not had any complaints from them. I have had a fair share from those who were designated as the extramural labs—.

Ms. LOFGREN. Well, I think their concern is that they will not be able to compete—I mean—.

Mr. MCQUEARY. Well, they will not be able to. That is the—.

Ms. LOFGREN. If—for example, I mean, you have got—without naming names, some labs where, I mean, the depth of the scientific experience is just breathtaking. I mean it is awesome.

Mr. MCQUEARY. In many cases, yes.

Ms. LOFGREN. And so they are the intramurals, but we are going to deny the best scientists in their field, maybe in the world, the opportunity to actually do work for us later.

Mr. MCQUEARY. Well, at the same time we have these views coming from the private labs, we also have a university and a private sector who looks at the labs as their competition.

Ms. LOFGREN. Right.

Mr. MCQUEARY. And a view that the labs have, well the insight into what the government wants to do, and therefore, they have the added advantage, and so we have been trying to do a—what I will call a balancing act—.

Ms. LOFGREN. Right. But—.

Mr. MCQUEARY. —to work something out, but excuse me.

Ms. LOFGREN. But our job is to get a job done, not to be a jobs program, right?

Mr. MCQUEARY. Absolutely right. And I completely agree with that, and in fact, you raise a point, if I may make it here, the amount of money that Science and Technology will spend in all of the labs on what I see as an ongoing basis, is about $200 million. DOE spends almost $9 billion, or they have a total budget on those labs of almost $9 billion. The Department of Homeland Security has about another $100 million, the balance being spent primarily in other directorates, Borders, and Transportations, so there is about $300 million out of $9 billion, so we represent 3 percent of the total budgets they have got.

And had we gone down a path of let us just put some of this in all the labs, it is my professional view that we would have such a small amount of money in any lab that it would be difficult to get the needed attention that we have to have on ours, other than

through, you know, Congressional direction or something of that sort, and that is not the way to get scientists to perform.

Ms. LOFGREN. So, I will stop, because I—we will have a second round, but—.

Mr. MCQUEARY. Okay.

Ms. LOFGREN. You are not planning to change this intramural, extramural—.

Mr. MCQUEARY. Oh, at the—I had testimony before Congressman Boehlert's Committee the last week or week before, time runs together for me.

Ms. LOFGREN. Yes, it does.

Mr. MCQUEARY. And what we agreed to do is have an independent review team. I volunteered to have an independent review team to look at the methodology we had used to make the selection, because there was nothing magical about it, or intended to be surreptitious, and so I would be have it examined, and we will see where we go from there. Another—and we will look at options. We could make them all—as a possibility, although I would rather not do that today. I wouldn't do it today. It could all be intramural, but with that goes the requirement that they not be, as they get access to inside information, then they cannot compete, as I would see it today, because I view—that would be against fair competition with private industry and not something—a direction we should go in.

Ms. LOFGREN. We will have greater discussion on this.

Mr. MCQUEARY. Okay.

Ms. LOFGREN. And I—.

Mr. MCQUEARY. Sure.

Ms. LOFGREN. I am a big fan of the private sector, as you know, but I also think that you would be hard pressed to find the depth of science, and anybody in industry will tell you the same thing, in the private sector that you will find at some of these labs in some of these specialized subjects. I mean, it is just—.

Mr. MCQUEARY. In some areas, you are absolutely right.

Ms. LOFGREN. That is why we have the arrangements that we do to roll their science out into the private sector. I mean, there are really gems, national gems.

Mr. THORNBERRY. Completely agree. Sometimes, I think if nobody is happy, that you have hit on a pretty good mean, but I don't know if that is completely true. The gentleman—.

Mr. MCQUEARY. That was not my intent, but—.

Mr. THORNBERRY. The gentleman from New Jersey.

Mr. ANDREWS. Thank you, Mr. Chairman. Thank you, Secretary McQueary, for an excellent job testifying and for the written materials as well. I too appreciate the establishment of benchmarks and measurement parameters, so we can see how you are doing, and so you can see how you are doing. I have three questions.

The first is about biowatching. To the extent that you can tell us without breaching any classified information, was a Biowatch facility used in the Senate Office Building when the ricin incident occurred?

Mr. MCQUEARY. No, sir. It was not.

Mr. ANDREWS. Was there a reason?

Mr. MCQUEARY. We did not—ricin is not something that would be detected by Biowatch, and I would rather not go into much more detail, but we could certainly have a classified discussion about—.

Mr. ANDREWS. Is it one of our goals to develop technology that would make ricin identifiable?

Mr. MCQUEARY. Ricin is readily identifiable if you begin to look for it, as I am told. I mean, my understanding of the details of the science, but the difficulty isn't—is not in identifying it, as we saw when the first indication, whether we have a scientific method of being able to determine, independent of human intervention, I can't answer that question, but I will be happy to—.

Mr. ANDREWS. I understand.

Mr. MCQUEARY. —determine whether there is something and provide an answer for it.

Mr. ANDREWS. The second issue is about standards. I think among the most important tasks among many important tasks that your agency has is to develop good, clear, high standards, and here is the measurement parameter I, in my own common sense, would have used to measure that. No doubt, somewhere in America today, some Port Authority executive is being approached by a vendor who wants to sell her or him a radiologic dirty bomb detection device, and the vendor will do a PowerPoint presentation and have a slideshow and a CD–ROM they could leave behind that says how well it works.

Two questions. Does the Port Authority executive, under the law that we are working under, have the obligation to refer to standards that you have created, and second, have you created standards to which the Port Authority executive could refer to determine whether the product is workable or junk?

Mr. MCQUEARY. It is very difficult to tell whether it is junk, because junk is sometimes in the eye of the beholder. The—we do have standards that we are considering—.

Mr. ANDREWS. Shouldn't you be the—we want you to be the beholder.

Mr. MCQUEARY. Okay. All right. Fair enough. We do, indeed, have standards for radiological detection devices. We have issued those standards, and they are available. The methodology that we propose to use for states and locals that would buy things for which we do provide standards, and we have many that we have to do, would be in the grant program that we have, we will specify, that is administered by Office of Domestic Preparedness, we would specify the types of equipment that should be purchased with that, and we believe that that will be motivation, because I can assure you at least in our interaction with state and locals, they are anxious to have standards from us. They are anxious to have equipment be interoperable.

Mr. ANDREWS. Are we at the point where those standards are now being included in the contracts for the grant agreements to these local recipients?

Mr. MCQUEARY. Yes, sir.

Mr. ANDREWS. That is great.

Mr. MCQUEARY. We have included—for the radiation detectors, and—.

Mr. ANDREWS. And I assume that that is on a continuously upgraded basis, as we learn more about these detectors, the standards will rise.

Mr. MCQUEARY. That is correct.

Mr. ANDREWS. So something that meets the standards in 2003 may not meet it in 2006, because we can do a better job in 2006.

Mr. MCQUEARY. Right. And that is the very nature of standards, but you have a body. We of course use the National Institute of Standards and Technology as well as ANSI and other standard agencies. We are—we have not become a standards agency. What we have become is a stimulator—.

Mr. ANDREWS. Right.

Mr. MCQUEARY. —of other organizations to help us prepare standards for areas that are technologically—.

Mr. ANDREWS. I cannot emphasize enough how important it is that we broaden the substantive reach of those standards, and then increase the depth to which the standards reach, so that certainly no federal dollar is spent on unworkable technology.

Mr. MCQUEARY. Very important.

Mr. ANDREWS. And hopefully, eventually, no dollar, private, public, federal, or local, is spent on such technology. The world, as Congresswoman Lofgren said, is just filled with charlatans right now. You know, two guys who can string together two soup cans and some fishing wire and call it a telecommunications system, and it is very important for reasons of protecting the public and protecting the public's wallet that we not secede to that wish. The third question is about standards in cybersecurity. What is a realistic expectation for a year from now for us to expect from your agency in stimulating standards in the area of cybersecurity. What would be a successful 2004 for your agency?

Mr. MCQUEARY. The—excuse me, the area of cybersecurity, as we all know, is a very complex one, because of the high degree of complexity of the Internet and all the interactions that that entails. Whether we can actually develop standards that will be—that we can point to in a year's time, I could not answer that question, and it would be inappropriate for me to even try to do that, because I don't think we are far enough into this. We do have the National Standards—the National Cybersecurity Division that has been formed as a part of the information analysis infrastructure protection, actually particularly reporting into—to the Assistant Secretary Liscouski. I believe that is the right place for it. We have a close relationship with the Director of that organization. In fact, I have a person dedicated full-time to working with that organization, so that we can help them from a scientific perspective understand the kinds of things that we need to do. We do have a couple of programs underway with the National Science Foundation, and the National Institute for Science and Technology that deals with cybersecurity, but I think it is premature for me to try to speculate on what we can actually do in a year's time, because of the complexity."

Mr. ANDREWS. Thank you very much. Thank you, Mr. Chairman.

Mr. THORNBERRY. I thank the gentleman for his questions. The Subcommittee has been joined by the full Committee Chairman,

the gentleman from California. Does the Chairman wish to be recognized at this point?

Mr. COX. I thank the Chairman. I would like to also thank Dr. McQueary for joining us today, and before I put just one question, I would like to acknowledge that this is the one year anniversary of the Department, and in particular, I would like to acknowledge the progress that you have made in your area of responsibility. You haven't even been there for a full year, if I am not mistaken.

Mr. MCQUEARY. That is correct.

Mr. COX. And so, the amount of territory that we have covered in a very short period of time is just absolutely extraordinary, particularly when we think that your responsibility, unlike some of what comprises Homeland Security, the merger of preexisting agencies, your responsibility is to create this S & T Directorate from whole cloth, and so it is truly formidable. I want to congratulate you on your successful implementation of Biowatch in 30 cities. I want to thank you for getting the SAFECOM program online, so that we can help our first responders with interoperability. I want to thank you for generally improving the flow of technology to our first responders, and finally, I want to thank you for your contribution to a metrics based strategic plan, the top line abstract of which we received here in Congress yesterday.

Second, I want to let you know that there is significant support on both sides of the aisle on this Committee for the President's budget for R & D investment for S & T within the Department. The President's fiscal year 2005 budget proposal, across all of our Federal partners, is increasing R & D investment by 44 percent over 2001 levels, and that is going to take us to $132 billion next year alone.

The commitment to Homeland Security, I think, is very clear, because your Homeland R & D budget is the largest increase of any executive branch agency or department. You are going to get—if the President's budget actually becomes authorized and appropriated, 15.5 percent, in Fiscal 2005, so I think that reflects the properly—support, not just in the legislative branch, but throughout the executive branch and at the White House as well, the strong support for your mission.

The question I want to put to you concerns the Safety Act. The Safety Act, of course, which was part of the Homeland Security Act, is meant to provide some legal certainty for people who are developing and then deploying technology that can protect us from terrorism. It puts them in the crosshairs from a liability standpoint, because by definition, if this equipment is ever going to be useful, it is going to be useful in an event of mass catastrophe or mass murder or some really awful calamitous event, and when bad things happen, lawyers are sure to follow. We want to make sure that, you know, to the extent that people are following all the rules in the law that they are getting the protections of the Safety Act, which doesn't immunize them from lawsuit, but at least gives them some certainty, and that received, as you know, bipartisan support when we put it into the law.

One of the responsibilities of your Directorate is that you are going to prioritize the applications under the Safety Act. We have got a website that is up, and the data that I am looking at here

indicate that you are getting about 2,000 hits a week on this website, but we have only had 9 full applications under the Safety Act, and 5 of those antedate the website being up. We have only had 31 pre-applications, and there is some indication that part of the reason that this is so underutilized, and we are not bringing anything through to fruition, because nobody has been approved, is that there might be some undue burden, or we have got some barriers to entry here.

There have been some expressions of concern about speculative questions, particularly regarding potential liabilities surrounding events in which these technologies might be used, and I know that it is your interest in avoiding any unintended burdens on applicants. So I am wondering what the Directorate can do, and what you have in mind to do, so that we can be a little more aggressive in implementing this part of the Act, and get some leverage so we can realize the Act's intended benefits.

Mr. MCQUEARY. The—well, the points you raise are very important ones, and as you well know, we issued the Act on an interim basis. It is still an interim Act at this point, and I believe it is March or April before we would expect the final version, and the intent of that all along has been to get as much feedback from industry and people who have an interest in this to try to make it be as—not have it be onerous in any way. Now—and we—the inputs that we primarily had, so far, some people still believe that it takes more time to fill out than the others, we have asked in each instance where people have submitted full applications, to give us their estimates as to how much time was spent, so that we can get a sense of what it is. That is one thing, and as I understand it, we have not had anyone coming back in a formal sense and telling us what they have actually spent on that.

The other thing that we have asked to do is to visit—have some of our professional people out of the SAFETY Act Group visit with each one of those who have submitted a formal application, and review in detail what their issues are, so that we can try to move in a direction for making this be as simple as possible, because we—I completely agree with you. It needs—I think it needs to be thorough and professional, but it does not need to—we should not have it be overly burdensome and complex. We do have a difference in point of view within our people who put together the—request the information as to how complex it is, versus what some have said, and I think we need to reach closure on that, so we have a common understanding, and that is the path we are on right now.

Mr. COX. Well, I thank you, Dr. McQueary, and I thank you, Mr. Chairman. I yield back.

Mr. THORNBERRY. I thank the Chairman. The Chair recognizes the gentleman from Texas, the Ranking Member.

Mr. TURNER. Thank you, Mr. Chairman. I was just thinking, as Chairman Cox was complimenting you on your progress, which we are all pleased with, that he probably didn't understand that as a graduate of the University of Texas, that should be expected.

Mr. MCQUEARY. Thank you.

Mr. TURNER. One of the areas that I have had some concern about, Dr. McQueary, is the fact that when we look at your budget as a whole, the lion's share of it is directed toward bio-counter-

measures. We all know this is an area of great threat and need, so I don't mean to be critical of the commitment that we have made there, but as I look at some of the other areas, I am not sure that we are doing as much in some of these other areas as we need to be. We all know that we haven't yet completed this task within the Department of having this comprehensive threat and vulnerability assessment, and I think the head of that Directorate, a few months ago, said it might take 5 years. I talked to Admiral Loy the other day. He said no, that wasn't the date. That was unacceptable. It needed to be a lot shorter, and I urged him to continue to pursue that aggressively.

In your written testimony, you set forth nine factors that your Directorate considers in prioritizing research and development activities. The sixth factor is a current threat assessment, as understood by the Intelligence Committee. The eighth factor is an expert understanding of enemy capabilities that exist today, or that can be expected to appear in the future. Both, obviously, are very critical and important factors, but in the absence of a completed, comprehensive threat assessment, please give us some feel as to how you interact with the IAIP Directorate in trying to discern those two factors, and make decisions with regard to allocation of budget requests.

Mr. MCQUEARY. The—that, of course, is one of several factors, as indicated in the testimony, that we use, and ultimately, we have professional people who—that are on the S & T staff, that take all of these inputs, and then render a judgment based upon their experiences and knowledge about the science involved, as to ultimately where we should be spending our money. The interaction with the IAIP group, I mentioned earlier, we have an individual in the cybersecurity area as the lead Director for our interaction in that area, dedicated full-time to working with them. We have another group of people that work in the critical infrastructure protection area, and at least one of whom is in residence virtually full-time at the Naval facility on Nebraska Avenue there with the IAIP people. So, it is very much a—what I will call a human-to-human interaction and discussions among professional people, to help us render those judgments that we have to make, because we don't have any—I don't have a matrix, for example, of—I weight the nine different areas I mentioned, 1 through 10, and somehow end up with a numerical figure, and say, well, this tells me what to do. Ultimately, scientific judgment, and this is true no matter whether it is government or private industry. Smart people have to look at the circumstances and render judgments, and what you—we expect is to have them be right most of the time, and in this case, they need to be right all of the time, so—.

Mr. TURNER. What concerns me is that without that comprehensive threat and vulnerability assessment, in many ways, we are kind of operating ad hoc with regard to where we ought to spend our dollars. I know the bulk of the increase in your budget this year, the budget request, is in the bio-countermeasure area. In fact, I guess if you took that out, your budget would probably be about level funding from 2004. So, if I am looking at the right line here, there is $407 million in the bio-countermeasures area.

Mr. MCQUEARY. Yes.

Mr. TURNER. But when you look at cybersecurity, which we all know is another critical vulnerability, if I am reading your budget request correctly, it is $18 million.

Mr. MCQUEARY. Yes.

Mr. TURNER. And I am just not certain that I feel very comfortable with the process that leads us to the conclusion that $18 million is sufficient to deal with the threat in the cybersecurity area. Tell me how you feel comfortable with that.

Mr. MCQUEARY. Well, as you probably recall, we had $8 million in there, and the first time I came before this group, and I certainly—I remember Chairman Cox and I am sure many others, pointed out that was inadequate. At that time, we did not have the National Cybersecurity Division in existence, and the Infrastructure Protection Group. We now have that. I believe they have a target. I have forgotten what he—I actually do not remember the budget that he has. So I view our $18 million as a supplement to the primary focus that is in the National Cybersecurity Division, and our job is to provide the R & D support for them, and based upon where we are right now, I am comfortable with that. Should we conclude that that was not the right amount, I would have no hesitancy to come back before this committee or any other that I deemed appropriate to ask for reprogramming if that were the case.

If I may address the biologic area, would you—if I could just give you the—.

Mr. TURNER. Certainly.

Mr. MCQUEARY. —thinking on that. The way we—the biologic threat is what we refer to as a temporal threat. The other threats that we deal with are spatial threats, and what I specifically mean by that, the criticality for the biological threat is to be able to determine that something has occurred, and do that quickly, so that one can implement the necessary measures in order to try to deal with whatever that might be.

In all the other threats, we know when that event has happened, whether—all the way from a nuclear bomb to some kind of dirty bomb, if you will. So you know where—and you know pretty much what the containment areas are, and so we understand what we have to do there. The way we determine where the money should be spent is by considering two critical factors. One is what is the magnitude—how severe is the threat, and certainly nuclear, in terms of the devastation it can cause, is very, very high—has a very high "number" associated with it, but there is also the factor of what is the probability or likelihood that that event will occur. And you—when you look at the biological threat, the devastation that can be caused in the biological area is extremely high. The ease with which someone can inflict devastation upon this country is very easy, and therefore, from the standpoint of the place where I believe with all my heart and soul, where we need to spend a great deal of our effort and focus our attention is in that one. We don't do it at the exclusion of everything else, but I truly believe that the vulnerability in this country lies in the biological area as much as any, in terms of devastation of the country.

Mr. TURNER. When we heard that the Department was going to create a DARPA-like entity, most of us had in our minds that it

would be for longer-term or advanced research kind of efforts. As I understand it, HSARPA, within your umbrella, has evolved more to deal with shorter term projects. I can understand the need for it, but I do regret that we still haven't been able to see a full advanced research agency similar to DARPA arise within the Department. Could you share with me your thoughts on that subject and what hope we might have for moving to the more advanced research kind of concept that we all thought we were creating initially?

Mr. MCQUEARY. Okay. I certainly will, because I view that I am responsible for the path that we are going down. As I got into this job, I—when I first took it, and probably, when I met with you in May of last year, if you had asked me what do you think your job is really going to be, I probably would have said I think setting the scientific direction that we need to go so we can determine what research areas we need to go into in order to make this country safer.

After I once got into the job, and we began to see all of these interactions with companies and universities, and the labs, as Congresswoman Lofgren mentioned earlier, it became readily apparent to me that there is far more technological capability that exists in this country than we are taking advantage of, and so for us to launch onto a path of why don't we do more research before we determine how effectively we can use that which already exists, in my judgment, would not have been a proper course of action, number one.

Number two, I think in view of the vulnerabilities that we have, it behooves us to spend money to try to make corrections today, if you will, today, tomorrow, short term, near term, in areas, and that is why I—that is the reason we have gone down that path. I believe over time that what we will do is evolve into more fundamental research, and so you will see a different balance. We are at about 10 percent in that range, 8 percent, I believe, fundamental research proposed in fiscal year 2005, and I would expect, over time, that will move in the direction that you have suggested, and appropriately so.

Mr. TURNER. Thank you, Doctor.

Mr. THORNBERRY. I thank the gentleman. Dr. McQueary, just a stray thought that occurred to me. I am interested in your distinction between temporal and spatial. It may be that cyber has elements of both. They don't call them viruses for nothing, and it is interesting, because it may be a hybrid of some of the things, and we can talk about that later. The gentleman from North Carolina is recognized.

Mr. ETHERIDGE. Thank you, Mr. Chairman. Okay. I want to make sure we are on the same—Dr. McQueary, thank you for being here today, and thank you for your testimony, and as a former resident of the state of North Carolina, you probably, as well as anyone in this room, know that our state has had an awful lot of experience with natural disasters, especially floods and hurricanes that have been particularly devastating to our agricultural sector in North Carolina, and consequently, the state has developed a great deal of expertise, really, in this whole field of agricultural disaster planning, response, and recovery. And last year, the Association of

Food and Drug Professionals, with the support of a number of Federal agencies, for officials, strongly encouraged the North Carolina Department of Agriculture and the Consumer Services area of that, along with the—a number of other agencies, to develop a national model for food safety and security systems. In response, the Governor easily established the North Carolina Food Safety and Security Taskforce, headed by Dr. Tom McGinn, the state veterinarian, who I am sure you are familiar with. This multi-agency group worked together for months, and worked to provide a comprehensive planning and response initiative, and it is entitled the North Carolina Food and Safety Security Project.

It is now ready for implementation, and I am told by folks at the state level, because it is in this form, they didn't have the money to finish the work, but what they have done is shared it with a lot of other states, that are now looking at it. It is developed so that it can be implemented, and I am informed that they can't afford to shoulder an entire $6.8 million cost of the Federally requested program, and I understand that they have—they are not eligible, apparently, for any DHS grant funding, in the definition of DHS grant funding, but it is obviously a project that was asked to be done, and it would be of benefit to every state in this country, because as you well know, agriculture now is a $1 trillion industry—.

Mr. MCQUEARY. Sure.

Mr. ETHERIDGE. —in this country, and the safety of it is very important. And I guess I am asking, and you might not want to answer today, but maybe have someone on your staff, is there any opportunity of assistance from S & T Directorate for some funding that could be used, that we could identify, because it is a piece that was asked to be done, and we could use it to share with other states, because I think it—this is the kind of thing that we ought to be working together to get done.

Mr. MCQUEARY. One thought that comes immediately to mind is that we—and I hope that the group has been—has submitted a proposal to be considered for our—I guess our third Center of Excellence, because that is an area in which we specifically are dealing with post-harvest food safety, is the purpose of that third Center of Excellence, and we have been out—we have been on the street with the RFP, so I have not seen the names of the participants, because I have tried to stay away from—.

Mr. ETHERIDGE. Sure.

Mr. MCQUEARY. —knowing the name, but I think we—.

Mr. ETHERIDGE. But I think this is at the university level, where they are pulling together—.

Mr. MCQUEARY. Well, it is at the university level—.

Mr. ETHERIDGE. But this is a little different, in that it was agency generated at the request of the Federal Government, and I hope we have someone in your Department we can talk with about that.

Mr. MCQUEARY. I would be happy to—.

Mr. ETHERIDGE. Because I think that is something that we could use right away to make a difference, so let me move on—.

Mr. MCQUEARY. You can have them contact—.

Mr. ETHERIDGE. —to another one.

Mr. MCQUEARY. Have them contact me, and I will be happy to—.

Mr. ETHERIDGE. Okay.

Mr. MCQUEARY. —make sure that we take—.

Mr. ETHERIDGE. Fine. Thank you.

Mr. MCQUEARY. —a hard look at it.

Mr. ETHERIDGE. Let me get to know, is it in your written testimony, you say in 2005, the Emergency Preparedness and Response Portfolio will continue its focus on technological developments, and technical guidance for states and local first responders, one of the areas that has been alluded to earlier. Would you be kind enough to discuss the kind of focus you are talking about here, and give us some examples, if you have them, of the technology and guidance the S & T Directorate plans to offer to our first responders in this country?

Mr. MCQUEARY. In the area that we are currently working—in fact, we expect to make announcements, I believe it is on—that would be tomorrow, on some protective clothing standards, specifically geared towards first responders, and so that is a first step and something we are beginning, because that is very important. As you may or may not know, we—one of our first contracts that we let out of the Technical Support Working Group was to North Carolina State—.

Mr. ETHERIDGE. Right.

Mr. MCQUEARY. —to look at protective material, and so those are two examples of things that we have done. There is more to be done, but those are two that come to mind, and I could—I would be happy to take a look in more detail and provide more detail for you in the—.

Mr. ETHERIDGE. Let me thank you for that, because I have visited that site, seen that material, and for those who haven't on this committee, it is amazing what it does for protecting our first responders, and—not only in the fire area, but in—where equipment gets snagged and others, and I have another one. I hope when they get a second round and we will—thank you very much.

Mr. THORNBERRY. I thank the gentleman. The Chair recognizes the distinguished gentlelady from Texas.

Ms. GRANGER. Thank you, and thank you for being here. I have perhaps a statement more than a question. Some of us attended the National Defense University Tuesday morning for an exercise on cybersecurity, which is probably why you are getting these questions, and we left there, of course, with more attention to cybersecurity and the threat of cybersecurity and what it can mean to us. As we should be concerned, this is—what we should—be focused on, but when I heard you say, a question that said what can we expect in one year, and essentially, you said I don't know, and then the question was, well, if you don't know, then how do you arrive at $18 million, which is what we are seeing, the $18 million for cybersecurity R & D, and then some others, and the answer was well, if I need more, I can come back. That leaves me more concerned than I was when I walked in here, so I am going to say to you that that is there anything you can do to relieve that concern, and say "here is what we are doing in cybersecurity, and here is how we are going about it, setting the standards."

Mr. MCQUEARY. That is fair enough. We specifically have two programs that are being funded jointly with the National Science Foundation and the National Institute of Health—or National Institute of Health—National Institute of Science and Technology, and in those programs, if I can find my notes here, I—actually, what I would prefer to do, if I could, could I send to you a detailed response to your question there, because it is quite a drawn-out number of different things that we are doing. I have got some 18 different—I think it is 17 different things that are listed here that are involved, and I would be happy to provide you great detail what we are doing, and—.

Ms. GRANGER. If you would.

Mr. MCQUEARY. —welcome the response—.

Ms. GRANGER. And then also, more specifically, about how you arrived at the $18 million figure.

Mr. MCQUEARY. Sure. That is fair enough.

Mr. GRANGER. Thank you.

Mr. MCQUEARY. Okay. Thank you.

Mr. THORNBERRY. Gentlelady, yield back.

Ms. GRANGER. I do.

Mr. THORNBERRY. Just wasn't sure if she was finished or not. And Dr. McQueary, I think the whole Subcommittee, of course, would be interested in those answers.

Mr. MCQUEARY. Of course.

Mr. THORNBERRY. Because we have jurisdiction in both areas, and—.

Mr. MCQUEARY. Of course.

Mr. THORNBERRY. —are particularly interested in that. The gentleman from Texas, has a question?

Mr. SESSIONS. Yes, I am, and I thank the Chairman. Dr. McQueary, over the last few months and really years, we have heard a good bit about intelligence that has been gained as a result of our combat operations in Afghanistan and Iraq about the threat that existed within those countries. I am interested, and this is perhaps much like Congresswoman Granger's, this is a statement, not a question, but perhaps at some point, I am interested in the Department of Homeland Security utilizing what I think has been a very effective way to identify targets and people that are our enemy as it relates to cybersecurity.

We got to see the flashcards or the playing cards with their pictures and names on them, but from my bit of serving on this Committee, I have not gotten a sense or a feel that we really know a lot about exactly who, where, and what those people are who are our enemies, as they relate to cyberterrorism. And it is my hope that in the coming year, and if I am wrong, feel free to tell me, but I believe that we need to make sure that we know more about who the specific targets are, aimed at the United States, who these people are, and what we are doing to combat them, and I have found myself, find myself today in a position of seeing each one of you put together a new department that is amazingly, and I think credibly, full of substance of what you are doing, but I hope you are aiming downstream at some things that we may have learned from the military about how to know who and where and what to expect and done some intel on that, so really it is an observation, that you are

going to take the money and tinker and learn and, you know, the chalk and the marbles, and learn who people are. But this person on this on this Cyber—Science and Research Development Subcommittee would be interested at some point, if that is developed during the year. We learned the name Al-Qa'eda after the war, not before the war. We learned the name bin Laden—I think I heard about it first when the British Prime Minister talked about the Taliban and bin Laden, because they supply drugs, 80 percent of the heroin that is on the streets of Great Britain. I would like to become more cogent with the threat that is out there, who the people are, what they do, how they operate, even if it is on a privacy basis, because I want to know you know, too.

I thank the gentleman, and I yield back.

Mr. THORNBERRY. I thank the gentleman from Texas. Dr. McQueary, let me ask a couple questions about this coordination issue that I mentioned early on, and in your statement, you talked about, as is obvious, there are a number of Federal departments that have some work going on on, say, biodefense and biosurveillance, and in answer to one of the previous questions, I understood basically your answer to be we are working on coordination to—in getting our arms around what everybody is doing, and how they relate to one another, but the inference I took is we are not quite there yet. Is that a fair inference, as far as understanding what is going on and being sure that we are not overlapping, but also that there are not gaps?

Mr. MCQUEARY. Well, as you know, there is a substantial amount of R & D work that goes on in many different government agencies, so I don't know if it is ever possible to be completely current. Although—however, with that said, I do believe that we have established the relationships. We have a close relationship with Assistant Secretary Paul McHale's Department of Homeland Defense. We have quarterly scheduled meetings with his group, which I believe I talked about last time when I was here, something we started early on. We deal, of course, with the National Institute of Health, the Department of Energy, all of these.

Now, in terms of could you—if you said to me, show me your calendar and let me see all of these formally scheduled meetings, many of these are not in that nature, because the more important thing is to have the scientific people in the various organizations interacting, and I truly believe that that is the way that most information truly gets transmitted, not through formal documentation, and so when you find an area, when we find an area, our people find an area, in which it is apparent that we need to interact, that interaction is taking place, and that comes back to a point that I made in earlier in testimony, choosing good people who are committed to the work that has to be done, so that you can have confidence that they will do those, assure that we have those kinds of interactions, and I am confident that we have the people in the science and technology organization.

I am also confident that within the Federal Government, there is a huge support for the Department of Homeland Security and what it is trying to do, because the importance of the mission that we have to do. And we find that wherever we go.

Mr. THORNBERRY. I have no doubt that that is also the case. It just seems to me it is a pretty big challenge, considering how many different agencies are involved, to know—and as you said, it doesn't mean that there needs to be a lot of meetings and pieces of paper floating around, but you have to have some sort of idea what people are working on to—.

Mr. MCQUEARY. And we do have various technical working groups that are there, and I work closely with Jack Marburger, for example, at OSTP, and of course, he has the vision of across the government, of the scientific portfolios that we have.

Mr. THORNBERRY. The Homeland Security Advisory Council has recently been formed. Will they have a role in helping to set S & T's priorities, and where you put money, and so on.

Mr. MCQUEARY. The—I believe—the answer is yes, and I think the issue where the discussion comes about is on what is that role, as opposed to whether they should have a role, because I—if we weren't going to let them have a role in what we are doing, what is the point in engaging these people and using their time? We—I actually will be meeting that group the first time tomorrow. We had the individuals selected. We have 18 of the 20 selected, membership, and so I will be meeting with them tomorrow to get that kicked off, and so, I am very anxious to have them review, you know, what we are doing, how we are doing it, and offer their professional views, because we have people from all walks of the scientific life, if you will, that are on that Committee, and I would welcome the input. General Welch is the Chair of the Committee, as you probably know, and so I am looking forward to the interaction. I think it is also important that that group have a connection back into Secretary Ridge's Homeland Security Advisory Council, too, and that will be conducted through Drs. Jared Cohen and Ruth David will be the point of contact we will have back into the Homeland Security Advisory Council.

Mr. THORNBERRY. So they will go up to that other Council, but also, they will have direct access to you and can raise an issue if they think you are shorting cybersecurity, or whatever it is, they will be able to talk to you directly about that.

Mr. MCQUEARY. Yes, and we owe you a report at the end of each January on—their report on what their views are on what we are doing. We, obviously, do not do one this January, because the Committee did not exist at that time, but we will have a report next year.

Mr. THORNBERRY. And let me ask one other thing in this round. Are there R & D programs you know of now that have not yet been brought into the S & T Directorate which will be, at some point?

Mr. MCQUEARY. We identify three in the testimony, that—where we have made the transition, and that is included in our budget. We are not quite through with that process, with—and I am talking internal to DHS. We are not quite through with the process. I believe we know where those programs are. We have a draft recommendation to Secretary Ridge, since he ultimately makes the decision as to what would be transferred in. I do know that we have his full support on making that transition, and he has made it clear to the operational units that is the case, so I would expect

within probably three months, we can give you a much more profound answer to your question.

Mr. THORNBERRY. Something in addition to the three that are contained in—.

Mr. MCQUEARY. Yes, very definitely.

Mr. THORNBERRY. Okay. Okay.

Mr. MCQUEARY. In addition to the three.

Mr. THORNBERRY. I see. Thank you. The gentlelady from California.

Ms. LOFGREN. Just a few additional questions. They really mostly relate to how we amass the information that is available. First, that we find out what is out there, and then make use of it in a way that helps us. You, in your testimony, talk on page 10 about the standards for development of biometrics for precise identification of individuals, which I—is great. That is something I have been wanting somebody to take the lead on for quite some time. However—and you also mention some place that you are working in coordination with US–VISIT. However, I am aware that US–VISIT is proceeding with their own biometric standard, that I guess has not been developed by you, and certainly, the FBI is doing their own thing, and I guess the concern I have is that all of this stuff is moving ahead, and I understand it needs to, but we are going to end up with different biometric standards that don't have the benefit of what you were planning to do. So, how are you—what is your intention on getting your presumably excellent work that is yet to be done, actually adopted by the various segments of the government that need biometrics?

Mr. MCQUEARY. It has been an interesting prospect to create a new Science and Technology Division that is a service organization for—organization that has been in existence for many, many years, and are already underway with the programs. The approach that we chose to take in the beginning, in the formation of the Science and Technology group, was in those scientific endeavors that are—were already underway, to not try to take those over, because we were in a mode of trying to grow our staff. At the same time, we were trying to get our operational procedures in place, so what we did is choose to focus in the areas more in detectors and standards and things of that sort, that was not intrusive on existing programs. We did, however, have a role to play in the US–VISIT program, in that the Science and Technology organization contracted to have a systems engineer—a system engineering company, take over and provide some inputs into what was ultimately put out in the RFP for the development of that. We did not have great influence on it, but it was something that I felt very strongly. US–VISIT will have to evolve over time. It now uses two fingers, as you know, for that biometric. At some point, the data system becomes overloaded and two fingerprints are not adequate to be able to provide a full biometric identification, and so I see us needing to move towards more—certainly more fingerprints over time, and that will—and I am confident that will be done, and as we make those evolution, I think we will be having more—I am confident we will have more Science and Technology involvement in that program.

Ms. LOFGREN. So, basically you are thinking that that proceeds, but when you are finished, you might, for example—they might

want to add on an iris scan. There is a smaller data load there, and the reliability is at least as high, maybe a little bit higher than fingerprints, and it would be duplicative, but with the duplication, it would have a higher level of reliability.

Mr. MCQUEARY. And if we have done our job, they should be getting their scientific view on whether that is a good idea from the Science and Technology Directorate.

Ms. LOFGREN. And how do you plan to have them listen to you? Since they don't listen to us.

Mr. MCQUEARY. I can't comment upon that. The manner in which we try to make sure that we have close relationships. I have one of my—we have portfolios, which you probably read in the testimony. One of the portfolio managers is responsible for the direct interaction with the Borders and Transportation Organization. In fact, she came out of the Borders and Transportation—she came out of the old Customs organization to join us, because our plan all along was for the portfolio managers that represented the operational units, we wanted to get a person that came out of those units, so that one, that person knew the interoperations of that unit from which they came, and two, we would hope that they could be a trusted person to contact within Science and Technology by virtue of having come out of it.

Ms. LOFGREN. Let me ask about another sort of consolidation issue, and that is in the whole cybersecurity testing issue. I am aware that—well, let me ask you this. How many on-staff people do we have in that function, as compared to contractors? Do you know?

Mr. MCQUEARY. I do not know how many the Director of the National Cybersecurity Division has. I spoke with him recently and asked him—.

Ms. LOFGREN. Okay.

Mr. MCQUEARY. —the question, but I simply cannot recall—.

Ms. LOFGREN. All right.

Mr. MCQUEARY. —the answer he gave me.

Ms. LOFGREN. Well, they are doing some things, and we have got universities. I know that the University of California San Diego—.

Mr. MCQUEARY. That is—and Berkeley, also.

Ms. LOFGREN. —and Berkeley, and Carnegie-Mellon are doing some things. Some of them are under contract with us. Some of them, they are just doing on their own. They have come with—up with different analyses of what might happen in various scenarios. It looks to me that we are primarily—in your testimony on page 36 on the Internet Security Technology, focusing in on cyberspace, but there is a physical infrastructure element of vulnerability that I am concerned has just not been attended to by—because it has not been assigned to anybody, and that that is maybe not being integrated into the diverse analysis that is going forward, some by the government, some funded by the government, some just independent. How do we get our arms around all of this good science information and integrate it into what you are doing?

Mr. MCQUEARY. Well, I—my view is that the appropriate thing to do is to look to the science—the National Cybersecurity Division that is in the Infrastructure Protection Directorate. That is their

established responsibility. People like myself have a responsibility to provide the scientific support that they might need in order to do that.

Ms. LOFGREN. So we ask, I mean, not you.

Mr. MCQUEARY. Yeah, I am not saying ask them and not me. I am just saying that is the area of responsibilities as they have been currently divided.

Ms. LOFGREN. Okay. That is fine. If I could indulge the Chairman for just one final question. The RFP for the Homeland Security Institute requires that the contract management and all the full-time staff have to be in Washington, D.C., and my question is why are we limiting the universe that can respond to that RFP just to inside the Beltway. Is there a reason for that?

Mr. MCQUEARY. I wouldn't view it as limiting it at all. I view it as—I mean, many companies set up operations here in Washington when there is a need to have—.

Ms. LOFGREN. Well, but—.

Mr. MCQUEARY. —the interaction. It does not—.

Ms. LOFGREN. My understanding is that all contractor management and all full-time staff are to be located in the Washington, D.C. metropolitan area.

Mr. MCQUEARY. That is intended to be for the people that would be working in that Homeland Security Institute. That does not mean—it could be a larger company, it could be a university or a national lab or something of that sort, that had the—.

Ms. LOFGREN. What is the rationale for that?

Mr. MCQUEARY. Because the—we will have some classified material to deal with over time. We have a small amount right now, but the important thing is having that group, they will be involved heavily in systems engineering work for us. It is very, very important to have them close, so that our people can interact with them on an easy basis. Having somebody on the West Coast or Northeast or wherever, and where you have always got to travel in order to have a meaningful interaction, in my judgment, is simply not the most effective way to get the most out of them.

Ms. LOFGREN. So it is not that you have already decided who is going to get the—.

Mr. MCQUEARY. We have not decided who is—we have absolutely not decided who is going to get that.

Ms. LOFGREN. Thank you, Mr. Chairman.

Mr. THORNBERRY. The gentleman from North Carolina have additional questions?

Mr. ETHERIDGE. I do. Thank you, Mr. Chairman, and thank you again. We have, and I am sure other members have, too, is have several companies who—certainly in our district, because of the technologies you can appreciate, in the Triangle, and have some ideas that they want to share with the Department of Homeland Security, and in past hearings, we have been told that there is an email address that companies should use to submit those technology proposals. Although I hear from some of my constituents, number one, it is hard to find, and number two, even if they do send emails, they say they aren't getting responses. I don't know whether it is true, but that is what they tell me.

Mr. MCQUEARY. Okay.

Mr. ETHERIDGE. And I also note that from the DHS website, that you will be hosting an industrial forum here in March that will include discussions on how to apply for funding and for contracts.

Mr. MCQUEARY. Right.

Mr. ETHERIDGE. And the forum is here in Washington, D.C.

Mr. MCQUEARY. Right.

Mr. ETHERIDGE. And many of the small business owners, as you can appreciate, that will be a huge imposition, because they neither have the resources, in a lot of cases, don't have the staff, even though they may have some technical expertise. So my question is this. Do you plan, in addition to asking my first one, I hope you will respond to, do you plan to put this information on the website so it is easily accessible and understood by some of these small businesses?

Mr. MCQUEARY. The answer is yes. In fact, we are trying to make our website be the place for unclassified information, and most of what we do is unclassified at this point, so that people can go to it. My recommendation to you is to encourage them to go to dhs.gov, at that website, drill down on the Science and Technology area, and that—and you can find, I believe, everything that we are doing in terms of RFPs we are putting out, broad Agency announcements and so forth, because our intent is to try to make that be so that people could electronically get access to what we are doing. In the case of those that said you have submitted things, if you will give me the names of them, I will be happy to personally find out where those—why we have not responded, because I thought we had a process that assured that people would get a response, if it was nothing more than saying we have your proposal. We are looking at it, just so that people know that a human being has actually intercepted the correspondence.

Mr. ETHERIDGE. I promise you in the future we will keep a list, if they call. Are there any plans to—.

Mr. MCQUEARY. We have had an enormous number of inputs—.

Mr. ETHERIDGE. I know.

Mr. MCQUEARY. —as you might guess.

Mr. ETHERIDGE. And I understand that. Are there any plans to change the way the Directorate deals with unsolicited proposals from small technology companies? I assume you are getting a lot of those, and are there full-time staff devoted to the outreach to companies and societies, because there are a lot out there that do have ideas, and it seems to me that is an area if we aren't doing it, we ought to be giving some serious consideration to.

Mr. MCQUEARY. Well, of course, we have just started the SBIR program, as you know about, and that will have, I think it is $19 million or so, whatever 2.5 percent of our budget is. Associated with that program, we have gotten very good response from that solicitation we put in, I believe, we have about 66 that are going to be selected out of the I think 300 or so that we had submitted to us for that, so I think that is a good outreach. The unsolicited proposals, while we encourage unsolicited proposals, because you never know when you might get it, the—I would frankly say, the likelihood of someone sending in an unsolicited proposal about something that we had simply never thought of is not particularly

high, and so many of the unsolicited proposals do not get the response that—because it may not be an area that we are truly interested in right now, and so the better approach is to look for how unsolicited proposals can map into the areas that we have publicly identified that we do have funding established for and we are going forward in, but at the same time, I don't want to discourage people who had submitted unsolicited proposals, because you can't be sure that you are never going to get sort of the Rosetta Stone that comes in from that.

Mr. ETHERIDGE. I realize you get a lot of them, but if someone could just let them know you have gotten it sometimes on the unsolicited ones—.

Mr. MCQUEARY. That is—and my intent is to have—.

Mr. ETHERIDGE. —they would be very helpful.

Mr. MCQUEARY. —us do that.

Mr. ETHERIDGE. Okay.

Mr. MCQUEARY. Because there is nothing more frustrating than to not get any get of response there.

Mr. ETHERIDGE. And we lose the opportunity for some pretty creative people in the future may continue to participate.

Mr. MCQUEARY. Sure.

Mr. ETHERIDGE. Let me ask the final one, if I may. In the little time I have got left. The elimination of EPA Homeland Security Building Decontamination research funding, because in the budget, in the 2005 budget request, the elimination of $8 million in current year funding for work focused on the improvement of methods and setting standards for decontaminating buildings following a potential chemical, biological, or radiological attack, and the budget language is the complete elimination of Homeland Security Building Decontamination research. EPA will not complete its core responsibilities to provide scientific, defensible, and cost-effective decontamination methods, and forces it to disband the technical and engineering expertise that will be needed to address the known and emerging biological and chemical threats. If that is true, Mr. Secretary, if the EPA is no longer to carry out this research, will Homeland Security be continuing these activities within the Directorate, and if not, is it your belief and that of the Administration that issues regarding building decontamination research and that of the technical and engineering expertise that will be needed to address these known and emerging threats in the future, no longer will be needed?

Mr. MCQUEARY. I only recently saw that language, and I simply do not know what the thinking was that went into the change you have there. I would be happy to look into it and see—.

Mr. ETHERIDGE. Would you. Okay.

Mr. MCQUEARY. —what we can find out.

Mr. ETHERIDGE. I would appreciate that.

Mr. MCQUEARY. And provide that information back to you—.

Mr. ETHERIDGE. Because I think this is one of those areas that somebody—.

Mr. MCQUEARY. The EPA does have the statutorial responsibility—.

Mr. ETHERIDGE. Sure.

Mr. MCQUEARY. —for cleanup. That is certainly true, and so I would assume that it is somehow embedded in that. We do not, for example, in Science and Technology, have any money that we are spending on cleanup—.

Mr. ETHERIDGE. Right.

Mr. MCQUEARY. —issues right now.

Mr. ETHERIDGE. But this is on preparing for what to do in the future, if you would look at that, I would appreciate it. Thank you, sir.

Mr. MCQUEARY. Yes, sir.

Mr. ETHERIDGE. Thank you, Mr. Chairman.

Mr. THORNBERRY. Thank you. Dr. McQueary, it occurs to me one of the first things that this Subcommittee did last year was to try to have a workshop for members and staff about dealing with the Department, you know, we have developed—you have developed a lot since then. It may be a useful thing to do again at some point, and maybe you need to have the conference in a couple weeks first, and—but we might set up some sort of an informal briefing, because the better we can help guide our constituents, and inform them, the better—the less hassle, I think, you all will have to deal with, and the more informed they are about how to deal with the Department, or access the Department, I think it would be easier on everybody. We might think about that. It is not all your Directorate. There are, you know, it cuts across a number of directorates, but it just occurs to me with some of the questions that we have had, that we may want to think about doing that.

Mr. MCQUEARY. We would be happy to take that on as a—to look and—if you maybe some of your staff members contact us, and we could work with them to see what—in more detail, what your interest is, and we could help work it.

Mr. THORNBERRY. Great. Thank you. The gentleman from Texas have additional questions?

Mr. SESSIONS. I do not, Chairman, thank you.

Mr. THORNBERRY. Let me ask, I don't want to put you on the spot, because this is an unclassified setting, but I wonder, I think it would be helpful for me to kind of have the view from 30,000 feet of where we are in certain key areas where we are trying to develop technologies that help make us safer. For example, patrolling, guarding our borders. And the kinds of—I guess what I am interested in, or—do we think there are some technologies out there that we just need to get fielded and we can make substantial improvements? Are the technologies not developed enough yet? Do we need to do a lot more research before we are ever in the ballpark? You know, kind of where we are with—in some of these areas, and I will throw that out to you, guarding the border as one. From your standpoint, without being too specific, where do you think we are?

Mr. MCQUEARY. Well, there is certainly plenty of work to be done, because we know there are people crossing our borders every day, illegally crossing the borders at places. The one area where I believe there is great promise is in the area of unmanned aerial vehicles. We do have some testing that has gone on already. We are beginning to do more. In fact, I—the lady who manages my Borders and Transportation portfolio that I touched upon earlier

has the responsibility from a Science and Technology organization to—and interfacing with the BTS organization and planning and executing that. Where we go with that, there are some—it is not clear yet. There are issues associated with aircraft flying and safety issues when you are around aircraft that has people on board and things, and all of that has to be worked out. However, I am confident that is an issue that can be worked. It is not—but it is something where you have a number of factors to consider, so it is—it would be my view that unmanned aerial vehicles and associated sensors, whether they be video sensors, or whether they be infrared, things of that sort, really offer the greatest opportunity for being able to provide information. The other thing would be if we can look farther into the other country, things are coming, so that you can anticipate. That sort of goes in the same category of what we are talking about. That is where I think there is a great emphasis, and I think also the President's proposal on how we deal with immigrants that are in this country now has a great deal of merit in helping move in the direction of solving some of those issues.

Mr. THORNBERRY. Thank you. That is exactly the sort of view that is helpful to me. Let me throw out another area. What about technology at border crossings? And obviously, there are a number of things that you are working on, but it looks to me like that we are pretty far along with the technology. It is just a question of making decisions, getting it deployed, and that sort of thing.

Mr. MCQUEARY. I think we are. I think the greatest challenge at the borders, as you probably know, is doing things that do not slow things down. I mean, there—we already have "congested borders," and I don't mean that a pejorative sense, but it is factually true, so if you slow something down a minute, well, a minute doesn't sound very much, but I am told that what you do is in effect cause the cars and trucks to begin backing up into Mexico or wherever it might be, where they are trying to come across. So whatever we do has to have an element, we need to do it reliably, and we need to do it quickly, and so that, I think, provides the—is where the great challenge is, because you can think of lots of things. I mean, you could say why don't we just take every truck and inspect every bit of it, and obviously, we couldn't live with that, so it is—whatever we do has got to be focused on doing it quickly, I believe. There are sensor technologies that are available, and how we implement those, I think, is a contribution that the Science and Technology group can make in concert with the Borders and Transportation people.

Mr. THORNBERRY. What about port security, particularly cargo shipments and trying to screen our cargo?

Mr. MCQUEARY. I mentioned the radiation detection work that we are doing in New York, and the Port Authority in New York and New Jersey. I believe that that work is going to provide a direction that we can go in to provide greater capability at the ports. I have also seen some interesting technologies that I don't have a scientific view yet as to whether they can be made to work, but I have seen some interesting technologies in what you could—conceive of doing a complete X-ray of a container as it is being taken off the ship, with the equipment on the crane that is lifting it, telemetry, the information from that scan over to a remote place,

have someone looking at it, and essentially in the time period it takes to be able to get it off. Now, this is the view of the contractor who has this offer. I have not rendered a complete view as to whether I think this could be made to work in a manner that could be afforded by the country. But it is an interesting concept, and there are others like that, too.

The key thing, though, I believe, is that we must do everything we can to try to know what is in the containers before they show up at our shores, and that is where it is very important to play the emphasis, because in your—if you wait until it shows up to shore, we are in a defensive mode then, and when you are in a defensive mode, it is difficult to always be right.

Mr. THORNBERRY. Where do you see us technologically at this point on the—in the biosurveillance area? It—you know, you have explained earlier its importance, and I think most people agree with you, it is, in some ways, the area of, I guess, greatest—I don't want to say greatest vulnerability, but when you put all the things together about the impact and the dangers and—it is on most people's—top of their priority list. Where are we in—.

Mr. MCQUEARY. I believe we know where we need to get to. I am very pleased with the manner in which Biowatch—we have had well over a half a million samples that have been taken by those sensors. We have yet to have our first false alarm in that, and that false alarms are a huge issue for anything in which you are dealing with the general public. It is very important not to continue to blow the whistle and say there is something there, when it isn't. We have had some detections that were made in Houston, which you probably know about, that were made on those Biowatch sensors. We actually picked up tularemia in the Houston area. It was not a terrorist attack. It was naturally occurring, as many of these pathogens are, and so I am pleased with what we are seeing in the performance.

The issue, though, is one of, I mentioned earlier, biological threats are temporal in nature, and therefore, we—right now, we go out once a day, sample these, take the samples. We then have to go and do the analysis on the samples, and so you could be talking 48 hours before you know that something actually happened. So, the ultimate detector that we need is one that makes a detection, does the assay in place, and sends a radio signal of some sort to wherever you might like to have it saying we have a detection. We have got a problem. And then you have got the measurement being made close to the event. And I believe—I don't believe that we are there scientifically yet. I do believe that it is an engineering problem, not a scientific breakthrough problem, and therefore, that is where the emphasis needs to be placed.

Mr. THORNBERRY. That is very helpful. Let me ask you about one other, interoperable communications, particularly of the first responders. We have had—the Subcommittee held a briefing on that last year, and it is a far more complex issue than one sees on the surface.

Mr. MCQUEARY. Yes, it is.

Mr. THORNBERRY. But where do you think the technology is on that?

Mr. MCQUEARY. Well, the—for—first of all, interoperable is a word that means many things. If you had 10 people in the room, and said please write down what you think interoperable means, it is very likely you would have maybe 9 or 8 different views on what it means. So it is really important, I think, to construct the language around what one means. The ultimate in interoperability would be where you and I are emergency responders. You have got your phone, I have got mine. We pick up and we can have an immediate conversation. We have got established protocols or overrides that might be there, so that because we are working in a threat condition, that we can assure that we are going to be able to have that communication. We do not have that right now. As we know, the—as in the south of New York, policemen, firemen can't even communicate among themselves. There are technologies that exist today, and if you read or heard Secretary Ridge's speech, he laid out what our plans are in dealing with interoperable communications. There are technologies where you can literally have an electronic box, if you will, and you have one phone, the simplest example, one phone communicates with a box, and then it can send out a—it can convert the signal into whatever format some other phone needs to have in order to have a conversation.

However, that means you have got this concentrator, if you will, which is not as efficient, nor will it be as cost-effective, but I do believe it is an important first step that we can take, and we can—and we do intend to provide standards associated with that. We are not quite through with where we want to be, but we will be providing standards that will be helpful to state and locals as they look at how they may want to spend grant money or—money. If you have not been to Chicago, and you get a chance to go, I would encourage you and other members of the Committee to take a look at what Chicago has done for its interoperable communications for the city. They have really solved the problem of how to communicate among all of their policemen, emergency responders, firemen, and they have a central control station, where people know what is going on throughout the city at all times among all of those, and so it is first-rate, but it is for Chicago only, and so there is more to it than just one city, but it is obviously a large area.

Mr. THORNBERRY. Great. Thank you. The staff has helped to remind me of one other area. I want to just see if you can tell us anything about in this setting, and that is the MANPADS issue, missiles which could be launched against airplanes. Do you—can you tell us anything about where the technology stands for dealing with that concern?

Mr. MCQUEARY. We—based upon what we have seen, as you know, we have awarded three contracts to three different views. We have—and each one of those contractors has an airline participant as a part of it, and I think that is a really important thing in order to give credibility to what gets done, because if the airline industry doesn't believe it, it becomes a very difficult thing to sell. I am confident that we are going to be able to identify a solution reasonably quickly. I know there are views that why don't we just take what is—some views, and why don't we take what the Defense Department has done and apply it on commercial aircraft. It is not that simple of a problem at all. I believe that within the time

period we have laid out, which is aggressive, within the two-year period, we can make a firm recommendation to the Administration and the Congress as to what the technical solution can be, and then a decision can be jointly made as to where the country wants to place the burden of that cost for making it happen, and I think that our job, I view, is not to make the decision as to whether to do it, but rather, to provide the technical wherewithal on which a decision can be made.

Mr. THORNBERRY. Great. I agree. Thank you. Ms. Lofgren.

Ms. LOFGREN. Thank you, Mr. Chairman. I—as you were talking, I was remembering the other questions that I forgot to ask. And really, there is just three, and they all really relate to the same subject, which is information that is out there in other parts of the Federal Government in some cases, that may or may not be known to you, because there is no good source. For example, as you were talking about the detection of bio-agents, I was recalling that the Post Office actually has deployed, and I know this, because one of the component parts is manufactured not in my district, but nearby, and I visited, where they do air samplings 24/7, and the component that is made in California actually does the testing for DNA of the biohazard. It produces a result that is 99.9 percent accurate, according to the Army—you know, they did a competition at the testing ground in under 35 minutes. So, I don't know whether that is the right—I mean, it was good enough for the Post Offices. They are just a component. It is a major defense contractor has got the prime contract, because they are testing for other things, but we don't need to invent that, because it has already been done, and I am—just one example, NASA is doing all kinds of interesting things, not for homeland security, for space, but they have, for examples, Ames has come up with a piece of equipment, at NASA Ames, where they can detect life, you know, in very dense rubble, and they were thinking it wasn't devised for rescuers, but that it would have an application for rescuers, but there is really nothing in place for the NASA Ames scientists to funnel that in to you, or the CIA, and they got so frustrated or alarmed about what was going on in Silicon Valley in terms of invention, I am sure you are aware that they hired Gilman Louie to be a venture capitalist, to go out and find out about this stuff. I don't know if Gilman gives reports to your department or not.

Mr. MCQUEARY. We have met with Gilman. I have not personally met him, but we have had people—.

Ms. LOFGREN. I see him on the airplane all the time, but he—you know, I mean, there is just—there is—but there is no real way to funnel this information into you, and I guess I am thinking. I don't know that I have the solution either, but there needs to be some thought given to how we harness the brainpower and diverse elements of the Federal Government, things funded by the Federal Government, so we don't end up reinventing what has already been invented.

Mr. MCQUEARY. I completely agree with you, completely agree with you.

Ms. LOFGREN. So what are your thoughts on how to do that?

Mr. MCQUEARY. Well, the—I certainly, at the top level, I think Jack Marburger, Dr. Marburger, is in the best position to have the

view of what is going on scientifically throughout the government. Now, he is one individual, and he has a relatively small staff, and so how much detail he can get into—.

Ms. LOFGREN. I don't think it is possible—.

Mr. MCQUEARY. —in order to be able to provide that, so—.

Ms. LOFGREN. —for him to play that ball.

Mr. MCQUEARY. —probably not. But other than that, I—the only way I know of is through working groups. By the way, we have had contact with NASA. I don't recall whether it was Ames, but early on, when I was reading all of the emails, I got an email from someone at NASA that had some ideas that I can't reconstruct at this point, as to what they might be able to do to help us. But that is informal, and it would be—I share your view that if we had a more formalized way of stimulating the interaction, we all could be better served by the money the Federal Government is spending, and I will take it on to try to see if I can come up with a better thing than saying why doesn't Jack Marburger help me.

Ms. LOFGREN. I would be very interested if you would give some thought to that, and maybe—.

Mr. MCQUEARY. Okay.

Ms. LOFGREN. —that is one of the questions we should pose to our Advisory Council as well. Thank you, Mr. Chairman.

Mr. THORNBERRY. Is the TSWG going to continue, or what is its role as you develop and move forward?

Mr. MCQUEARY. The TSWG has done a wonderful job for us, and I can't say enough, because we could not have launched our activity in May of this past year without their help, and so it has been really important for us to do that, and as you may recall, we had 3,344 white papers that were submitted at that very first TSWG announcement, and so enormous support there. We have support—we have funded them another $30 million in fiscal year 2004. The one area where I am looking for some change, and we are having a discussion back and forth. They are not able to move as quickly, for whatever reasons, as I would like to see us move. I think it is very important that we make our decisions, and get on with it, and MANPADS took us about three and a half months from start to issuance of contracts. We have been able to do similarly in chem-bio detectors, because of the OTA authority that was given by the Congress to be able to move quickly. So, I—it is an open question as to whether we will continue with the TSWG or not. Ultimately, I think it would be beneficial for us to have the capability, whether we have it indigenous into Science and Technology, or whether we have someone, some other agency manage it for us, it could be good, but I am—I would rather not give you a yes or no answer.

Mr. THORNBERRY. I appreciate it. I do think the ability to move quickly is just one of the essential elements for the military of the future, or for protecting our homeland.

Mr. MCQUEARY. Right. Absolutely.

Mr. THORNBERRY. I have got two or three more questions, but I would prefer to submit those for the record, and ask for a written response, and ask unanimous consent that all members have five days to submit written questions for the record, and to revise and extend their remarks. And if my colleagues have nothing else, let me thank you again, Dr. McQueary, for being here with us today,

for answering our questions, and for all of the work that you and your colleagues are doing to get this Department up and running and to make us safer day by day. We appreciate you.

Mr. MCQUEARY. We appreciate the support we receive from you, too, I assure you. And your staff does a great job in working with us.

Mr. THORNBERRY. Well, now, don't say that. They are going to ask for raises. But I appreciate you being here, and the hearing is now adjourned.

[Whereupon, at 2:43 p.m., the Subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE RECORD

QUESTIONS FOR THE RECORD FROM THE HON. MAC THORNBERRY

1. Developing meaningful metrics to measure progress in making the nation safer is difficult yet it must be done. What do you think are the most important indicators of your Department's success and what is the status of your efforts to develop a formal set of metrics?

Answer: In compliance with GPRA, the DHS has established performance goals and supporting performance measures for each of its programs. These measures are the most important indicator as they provide both macro and individual program status of success. For a macro view the DHS Strategic Plan provides the framework for carrying out the Department's Mission. Each program, and its associated performance goals and measures are linked to the DHS strategic plan goals they support. This linkage enables the department to collect information on progress in achieving goals and accomplishing the Mission of DHS. . . . *lead the unified national effort to secure America.* At the program level, the program performance goal and ensuing supporting performance measures provide consistent critical insight into the achievement of programs achieving their intended results. During fiscal year 2004 we began collecting quarterly performance results information on all our programs to monitor success at both the strategic goal and program level.

Although much has been accomplished, we recognize the need for continual improvement of performance measures. We have therefore planned further agency-wide training in developing better measures to be completed this year. This year performance information will further be refined by linking each program to DHS strategic objectives under each strategic goal, and development of additional performance measures as needed to reveal how each program explicitly supports each DHS strategic objective.

2. We know that the budget and planning is broken out by countermeasure portfolio. However, the implementation of the work is done by your four offices

- **Office of Plans, Programs, and Budgets**
- **Office of Research and Development**
- **Office of HSARPA**
- **Office of Systems Engineering and Development**

What are the budget breakouts for these Offices and how do they work together especially in getting technologies transferred to the end-user?

Answer: The fiscal year 2004 funds allocation by managing office is as follows:

Managing Office	FY 2004 Funds Allocation ($M)*
Office of Plans, Programs, and Budgets	118.6
Office of Research and Development	400.2**
Office of HSARPA (Includes SBIR)	246.5
Office of Systems Engineering and Development	108.7
Total	**874.0**

*Does not reflect fiscal year 2004 general rescission of $5.2 million.
**This amount includes $88 million for construction.

The Offices of the Science and Technology (S & T) Directorate work together through Integrated Product Teams (IPT). Membership from all of our Offices—Office

of Plans, Programs, and Budgets (PPB), Office of Research and Development (ORD), Homeland Security Advanced Research Projects Agency (HSARPA) and the Office of Systems Engineering and Development (SED)—participates actively in the planning and budgeting process through these IPTs. The IPTs for each portfolio work as a team to determine their mission space, their strategic goals for the next five years, and a list of prioritized deliverables. The executing Offices—ORD, HSARPA and SED—then respond to the prioritization process with programs that are subsequently executed.

The primary executors of the Technology Transfer function are the Offices of HSARPA and SED. When HSARPA or SED are assigned a project for demonstration and deployment by the IPT, that Office takes on full responsibility to ensure that all end-user requirements are met and that the technology delivered is affordable, manufacturable, interoperable, sustainable and easy to use.

3. The HSARPA has put out several Broad Area Announcements. Have the proposals received from these calls been reviewed, selected and funded by the HSARPA? What percent of the HSARPA budget is obligated at this time? What is the projected budget obligation by the end of fiscal year 2005? Is this process moving fast enough?

Answer: The Science and Technology Directorate is committed to ensuring technologies to secure the Nation are developed using the extensive resources, assets and experience of the private sector. Through the Homeland Security Advanced Research Projects Agency (HSARPA), the Directorate has already completed the selection process for two solicitations. Forty teams or individual companies were selected to enter negotiations from HSARPA's first research announcement (RA03–01, Detection Systems for Biological and Chemical Countermeasures) issued in September 2003. To date, eight teams are at work through an awarded agreement and all others were allowed to begin work through pre-award costs authorization. HSARPA issued its first Small Business Innovation Research (SBIR) Program Solicitation on November 13, 2003. All 66 winners are currently under contract.

Currently, HSARPA has four Broad Agency Announcements (BAAs) active and has publicly announced that in the next three months an additional five BAAs will be released. Additional solicitations are in preparation for late summer and fall of2004.

As of April 28, 2004, HSARPA has committed 84 percent of its allocated fiscal year 2003 and fiscal year 2004 budgets. HSARPA plans to have all fiscal year 2004 funds obligated by the end of the first quarter of fiscal year 2005.

The HSARPA solicitation process is moving at a rate commensurate with its allocated funding and staffing. As noted above, our process is accelerating.

4. As you know, this Committee has strongly supported the enactment of the Project Bioshield, which is unfortunately still pending in the Senate. However, as you also know, Congress has already appropriated hundreds of millions of dollars to develop and procure medical countermeasures for a variety of potential terrorist threats, whether nuclear, radiological, biological or chemical. Notably, this includes the $127 million for "nuclear and radiological countermeasures," $266 million for "biological countermeasures," $874 million for "general research and acquisition," and $890 million for drug development projects under Project Bioshield. These funds were intended to create a guaranteed funding stream to encourage the development of WMD medical countermeasures in cases where there is not likely to be any other commercial market for these drugs.

While we all would like to see the Project Bioshield legislation enacted tomorrow, can you please reassure the Committee that your Department, in conjunction with the Department of Health and Human Services, is moving forward to utilize these funds to get needed drugs for anti-radiation?

Answer: The Office of Science and Technology Policy (OSTP) National Science and Technology Council, Weapons of Mass Destruction Countermeasures Subcommittee, Radiological and Nuclear Threat Countermeasures Subgroup is the advisory committee that is providing priorities and guidance to Project Bioshield in the area of anti-radiation drugs. Efforts through licensure of these drugs may be provided by Project Biosheild funds. The funds available for the purchase of anti-radiation drugs are provided by the Strategic National Stockpile which is managed by an interagency group lead by the Department of Health and Human Services (HHS). The Department of Homeland Security (DHS) participates on this interagency group, which is currently developing a national acquisition strategy. Additionally, coordination of research and development (R & D) in the areas of both radioprotectants and radiation treatment drugs occurs on many levels including the

Counterproliferation Technologies Coordinating Committee (CTCC) and the development of the National Plan for Homeland Security S & T currently underway.

QUESTIONS FOR THE RECORD FROM THE HON. JIM TURNER

1. We understand that the Directorate is doing a strategic plan for fiscal years 2006 through 2010. **How will you prioritize resources over that period, and do you expect the distribution among the portfolios of biological, chemical, nuclear, and other countermeasures to remain the same as in the current budget?**

Answer: The S & T Directorate is currently conducting its fiscal year 2006 through 2010 Strategic Planning Process. Our planning process is centered around the use of Integrated Product Teams (IPTs). As mentioned above, IPTs are composed of representatives from each of our Offices, including the Office of Plans, Programs, and Budgets (PPB), the Homeland Security Advanced Research Projects Agency (HSARPA), the Office of Research and Development (ORD) and the Office of Systems Engineering and Development (SED). The IPTs for each portfolio work as a team to determine their mission space, their strategic goals for the next five years, and a list of prioritized deliverables. The Directorate's strategic planning and prioritization will be influenced by statutory requirements, national guidance, and user needs as well as subject matter expertise of our portfolio managers.

S & T's Corporate Review Board, composed of the Office Directors, reviews each Portfolio Plan and provides final S & T portfolio guidance regarding resource and program adjustments through a Decision Memorandum from the Under Secretary for Science and Technology. This Decision Memorandum, which may include shifts in budgetary priorities for the Directorate, will be issued in May, 2004.

2. Does the Directorate have a long-term list of the most important scientific innovations for homeland security? For example, are you looking down the road at handheld detectors that can identify all biological and chemical weapons? If so, how are research and development efforts being focused on these specific needs, as opposed to general work in their larger portfolios?

Answer: The Science and Technology Directorate recognizes that many organizations across the U.S. Government 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 that "The Secretary, acting through the Under Secretary for Science and Technology, shall have the responsibility for. . . developing, in consultation with other appropriate executive agencies, a national policy and strategic plan for, identifying priorities, goals, objectives and policies for, and coordinating the Federal Government's civilian efforts to identify and develop countermeasures to chemical, biological, radiological, nuclear, and other emerging terrorist threats, including the development of comprehensive, research-based definable goals for such efforts and development of annual measurable objectives and specific targets to accomplish and evaluate the goals for such efforts."

The development of this National Plan for Homeland Security Science and Technology is now underway. This National Plan will highlight the high priority areas and scientific innovations for homeland security in the short-, mid- and long-term time periods. The National Plan will incorporate much of the strategic planning described in the preceding answer.

3. Please provide additional information as discussed during the hearing on the plans to finish consolidating all Departmental research and development into the S & T Directorate.

Answer: The S & T Directorate is in the process of administrative actions and agreements that will establish management relationships with the following R & D activities within DHS:

- Transportation Security Laboratory (Border & Transportation Security Directorate, Transportation Security Administration);
- Customs Applied Technology Division (Border & Transportation Security Directorate, Bureau of Customs & Border Protection);
- Customs Laboratory System's Laboratories & Scientific Services Research Facility (Border & Transportation Security Directorate, Bureau of Customs & Border Protection);

- Immigration and Naturalization Services (INS) Forensic Document Laboratory (Border & Transportation Security Directorate, Bureau of Immigration & Customs Enforcement);
- In addition, S & T will establish management relationships with the U.S. Coast Guard R & D Center and with U.S. Secret Service Laboratory R & D activities that will take into consideration the traditional and protective missions respectively of these entities.

We will complete the administrative requirements to establish management relationships between these R & D activities and S & T by September 30, 2004. Our intent is to develop and expand collaborative relationships as these new management relationships are established.

To accomplish administrative actions to establish these management relationships, S & T is taking the following steps:

- The proposed management relationship between S & T and each R & D activity is being determined;
- Second, Memoranda of Agreement will be promulgated between S & T and each R & D activity; and
- Third, mutually agreed-to transition plans will be developed.

Forthcoming administrative actions will result in the formation of official management relationships between the S & T Directorate and each R & D activity in the Department and will address responsibilities for coordination and oversight of R & D activities as appropriate. Details of actions required to establish new management relationships and integrate R & D activities in the Department will be finalized by the Secretary.

4. How has the Directorate determined what areas are appropriate for university centers? After the next center on behavioral and social science studies on terrorism, what is planned for additional centers?

Answer: To date, DHS has established three university-based homeland security centers of excellence (HS Centers). The first HS Center awarded was the University of Southern California's Homeland Security Center for Risk-Based and Economic Analysis of Terrorist Events. DHS purposely focused the first HS Center in this area to validate models that may provide direct input on the risk and economic impacts of terrorism, which in turn help prioritize S & T's research agenda. This topic was also included in the National Academies of Sciences report, *Making the Nation Safer*.

On April 27, 2004, the Department announced awards to Texas A & M University and the University of Minnesota to lead two new Homeland Security Centers of Excellence (HS Centers) on agro-security. Texas A & M will lead the HS Center dedicated to the study of high-consequence foreign animal and zoonotic diseases; the University of Minnesota will lead the Center for Post-Harvest Food Protection and Defense. Both institutions have solidified partnerships with supporting academic institutions. Private industry will also be a partner with the University of Minnesota for post-harvest food protection and defense.

DHS has solicited input from the National Academies of Science, and considered Section 308, as amended, of the Homeland Security Act of 2002, to determine appropriate topics and prioritized areas for future university-based Homeland Security Centers. Having addressed countermeasures and cross-cutting portfolio needs in its first three HS Center awards and the forthcoming competition for a center in the social and behavioral sciences, an emphasis on research to support operational response is a likely direction for a future competition.

5. I am very concerned over the increasing use of security classifications and other labels (such as "Sensitive Security Information" or "Sensitive But Unclassified") to prevent dissemination of information that may not truly need to be kept from the public. Some in the academic community have found it so difficult to deal with these secrecy provisions that they give up on trying to work on homeland security issues. Do you share this concern? What is the S & T Directorate doing to make sure that areas of research that don't need to be classified are kept open? Is it possible to have portions of contract work be done under secrecy agreements without classifying the entire work?

Answer: The Science and Technology Directorate is committed to harnessing the vast resources our Nation's universities offer in the difficult challenge of protecting our homeland. To this end, the Department is committed to keeping as much research in the academic arena open to the public as possible. The S & T Directorate currently functions under the direction established by the 1985 National Security Decision Directive 189 (NSDD 189). NSDD 189 states that to the maximum extent possible, the products of fundamental research remain unrestricted. While future re-

search supported by DHS S & T may require classification, the Directorate remains committed to the tenets of NSDD 189 and will work to ensure that the portions of research activities that are fundamental in nature remain unrestricted.

6. I have heard from the academic community that there has been a fairly successful effort, called the Federal Demonstration Partnership, to standardize the process for applying for and administering grants and contracts. This process makes it much easier for individual researchers and universities to work collaboratively with the federal government. Will DHS be using the standard FDP mechanism for university centers and HSARPA work conducted at universities?

Answer: The Department of Homeland Security is not currently a member of the Federal Demonstration Partnership (FDP). DHS Office of Procurement is currently reviewing the FDP mechanism to determine if it will be a process that should be incorporated for university grants and cooperative agreements.

The S & T Directorate considers universities as an important part of the technical community available to work on DHS problems. The Directorate held a public workshop in December, 2003, specifically to understand the needs and outlook of the academic community. Participants from more than 100 universities and educational institutions attended the workshop. S & T solicitations have received good participation from universities at workshops, bidder's conferences, and at the white paper and proposal stages.

7. Under Project Biowatch, sensors are placed in cities across the country for the purposes of detecting airborne release of biological agents. This is a much-needed and profoundly locally-based federal program. Outside of the science, it seems the main challenge will be in coordinating with so many jurisdictions, the EPA as the owner of many of the detector platforms, and the CDC who arranges for the sensor testing. Does your Directorate have ultimate budget responsibility for the systems? And does that budget responsibility include the day-to-day operations incurred at the local level, or is that not covered by the federal government?

Answer: Yes, the DHS S & T Directorate has ultimate budget responsibility for the Bio Watch Program. The day-to-day operations and local expenses are funded by the DHS S & T Directorate as part of the BioWatch day-to-day operations. The BioWatch program currently does not fund local response activities related to a Bio Watch initiated event.

8. What will the activities and responsibilities of the National Biodefense Analysis and Countermeasures Center will be? How will its role differ from and interact with the activities of DOD and NIH? Does it have a role in Project Bioshield? What is the timeline for the facility's completion?

Answer: The National Biodefense Analysis and Countermeasures Center (NBACC) provides an integrated land responsive biosecurity enterprise that facilitates homeland security, law enforcement, and medical and veterinary communities' ability to understand, respond, deter and recover from the biological threats to the United States. This mission is critical to government policy and decision makers who manage national resources and programs to minimize human casualties and infrastructure damage associated with a deliberate attack with a biothreat agent.

NBACC directs and coordinates scientific efforts to improve our defenses against biological agents by gaining better information about current and future threats, understanding the risks associated with these threats, evaluating methods that may be used to deliver the threats, and conducting forensic analysis on threats to determine attribution. NBACC will develop a knowledge management system that integrates science, technology and intelligence.

Efforts undertaken through the NBACC will advance DHS S & T's close working relationship with the BioShield Program Office (Office of Emergency Preparedness, Department of Health and Human Services) to determine, validate, and prioritize biothreats as well as identify countermeasure gaps and guide biothreat countermeasure acquisition decisions. A coordinated decision process has been established whereby the Secretaries of Homeland Security and Health and Human Services make certifications and forward the purchase decision to the President through the Director of the Office of Management and Budget (OMB).

The NBACC concept is already being implemented through interim capabilities in science-based threat characterization and bioforensics operations and research, leveraging the U.S. Army Medical Research Institute for Infectious Diseases (USAMRIID)'s aerosol biocontainment laboratories and scientific expertise to accomplish near-term threat characterization objectives. Additional capabilities are currently being established through the Department of Energy National Laboratories'

research and development in information management, sensors, surveillance, and related areas; and through ongoing research and diagnostics work in the area of foreign animal diseases, a capability of the Plum Island Animal Disease Center (PIADC). The current estimated timeline for completion of the NBACC facility is mid-year of fiscal year 2008.

9. The budget request includes $129 million for "nuclear and radiological countermeasures," which I assume covers detection and treatment. Can you discuss the balance between detection and treatment? Also, how much is requested in the budget for antidotes for radiation exposure, which are generally quite close to market, compared to treatments for biological agents?

Answer: The budget for radiological and nuclear countermeasures includes all areas that must be addressed in conducting national research, development, testing and evaluation (RDT & E) to (1) prevent the importation of radiological and nuclear weapons and materials; and to (2) detect, prevent, protect against and respond to terrorist attacks. The balance between detection and treatment is critical and evolving. At present, the Science and Technology Directorate is in the early stages of executing programs and has sought to emphasize prevention. Hence, detection RDT & E is currently receiving the largest portion of funding. Under the Incident Management portion of S & T's Radiological and Nuclear Countermeasures Portfolio, assessment efforts for identifying the needed RDT & E for relevant technologies and treatments of radiation exposure is included and will soon receive funding. In the next few years, the balance between detection and treatment will change to put a greater emphasis on the Incident Management portion of the portfolio.

10. I commend you on the inclusion of 21 performance metrics in 12 categories in your written testimony, but there are no metrics on how well the Directorate is reaching out to the private sector to identify new technologies—the unsolicited proposals that are often the most innovative ideas.

There is, however, a metric for the numbers of new "technologies prototyped or commercialized." The goal for fiscal year 2005 is three. Can you describe what it means to have three new technologies prototyped and commercialized? Is this the same as saying that three HSARPA contracts are successful?

Answer: The DHS S & T Directorate, in coordination with the DHS Private Sector Liaison Office, has several sustained outreach efforts with industry. These efforts include multiple forums that provide for the exchange of dialogue between DHS S & T program managers and our industrial partners. These forums allow industry to better understand the future programmatic direction of the Directorate and provide an opportunity for DHS S & T Program Managers to learn about unique technical capabilities of industry and small business. Some of these conferences are focused on particular program areas, others cover many areas. The next of these broad conferences will be held July 12–15, 2004, in San Diego, CA. In addition, DHS sponsors a website for all businesses interested in submitting unsolicited proposals to the Department (*www.dhs.gov/openforbusiness*).

Among its first public gatherings, HSARPA hosted a Best Practices/Worst Practices workshop for industry and the participation was enthusiastic: 172 industry representatives attended. This event gave industry a face-to-face chance to explain their preferences for solicitations, awards, contract types, time schedules, and other administrative details, when working with the Science and Technology Directorate.

Complicated or extensive HSARPA solicitations are published first in draft form. This allows any potential bidder's comments to be read and reviewed before the actual solicitation is published. In this way, new areas of research can be identified and covered, recent commercial developments may be included, and realistic, understandable goals can be set in the formal solicitation.

Well before the first deadline for white papers, it is standard HSARPA practice to hold either a technical workshop or a bidders conference, or both. These public meetings establish common technical foundations, provide general and technical directions, and introduce the published solicitation in detail.

In addition, S & T solicitations executed by HSARPA provide a teaming website for the convenience of the smaller bidders who may not have the breadth of technical expertise in-house to compete for a full technical topic. This site facilitates discussion among potential bidders and promotes collaboration to achieve the challenging goals set by the solicitation.

Finally, the Small Business Innovation Research (SBIR) Program Manager not only manages the mechanics of the program, he is also the small business advocate for HSARPA research. An important part of his mission is traveling the country ex-

plaining the S & T Directorate's RDT & E program and providing hands-on help to small business. He explains to small companies with new ideas and concepts how to interact most effectively with the S & T Directorate. HSARPA has already awarded 66 Phase I (feasibility study) contracts to small businesses for research efforts in eight important areas. The next small business solicitation will be issued in May, 2004.

A successful prototype or commercialization is not the same as a successful HSARPA contract.

Typically, a new technology is developed and prototyped, then commercialized.

HSARP A contracts with the private sector for research that explores discoveries, expands original scientific work, or shows evidence of development potential. HSARPA also contracts for multiple technology development efforts. As development continues, prototypes are created in a laboratory to prove that the idea or concept can be physically constructed and made to work. The goal of development is to make prototypes that perform satisfactorily in operating environments.

Commercialization is bringing a capable prototype out of the laboratory into the commercial market for retail sale. There are many steps in commercialization. Systems Engineering and Development entrains mature prototypes and contracts for full scale engineering development and manufacturing engineering development activities necessary for commercial production. Development, proto typing, and especially commercialization take a long time, and multiple serial, parallel, and supporting contracts to do successfully.

Our stated goal is to have three technologies prototyped or commercialized in fiscal year 2005.

QUESTION FROM THE HON. KENDRICK B. MEEK

1. Mr. Secretary, how do you plan to execute the mandate given by Congress in the Fiscal Year 2004 Homeland Security Conference report regarding the participation of minority serving institutions (MSI) for DHS's University-based Homeland Security Centers program?

HBCU's have not historically received the sustained funding other institutions have received for infrastructure for research, particularly in the formula funding used to allocate federal and state dollars to land grant institutions. Currently, the federal funding disparity at the federal level has been estimated to be approximately 10 to 1 ratio or more between the 1862 and 1890 land grant institutions.

In the Fiscal Year 2004 Homeland Security Conference Report it stated "The Conferees encourage the Department to consider all colleges and universities that meet the requirements of U.S.C. 188 in the selection of university-based centers, including historically black colleges and universities, tribal colleges, Hispanic-serving institutions, and Alaskan Native-serving institutions."

It appears this language was implicitly suggesting that due consideration be given to minority-serving institutions or at least suggests that DHS should be sensitive to the historical significance of these institutions when designating centers.

Answer: DHS University Based Homeland Security Centers are selected through a peer-review merit-based competition, in which DHS openly solicits proposals to meet mission and technical criteria contained in a Broad Agency Announcement. DHS S & T invited representatives of minority-serving institutions (MSIs) to participate in the external peer review process, leading to the selection of an institution to lead a given Center. In addition, DHS S & T encourages institutions hosting Centers to establish collaborative relationships with other institutions, including MSIs.

○