HOMELAND SECURITY SCIENCE AND TECHNOLOGY: PREPARING FOR THE FUTURE

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, SCIENCE AND RESEARCH & DEVELOPMENT

of the

SELECT COMMITTEE ON HOMELAND SECURITY

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS
FIRST SESSION

MAY 21, 2003

SERIAL NO. 108–7

Printed for the use of the Subcommittee on Cybersecurity, Science and Research & Development and the Select Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE
97–119 PDF WASHINGTON : 2004

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., New Jersey
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

JOHN GANNON, *Chief of Staff*
UTTAM DHILLON, *Chief Counsel and Deputy Staff Director*
STEVEN CASH, *Democrat Staff Director*
MICHAEL S. TWINCHEK, *Chief Clerk*

SUBCOMMITTEE ON CYBERSECURITY, SCIENCE, AND RESEARCH & 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
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

MATERIALS SUBMITTED FOR THE RECORD

HOMELAND SECURITY AND TECHNOLOGY: PREPARING FOR THE FUTURE

WEDNESDAY, MAY 21, 2003

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 2 p.m., in room 2118, Rayburn House Office Building, Hon. Mac Thornberry [chairman of the subcommittee] presiding.

Present: Representatives Thornberry, Sessions, Boehlert, Smith, Weldon, Camp, Linder, Lofgren, Andrews, Christensen, Etheridge, Lucas, Langevin, Meek, Cox (*ex officio*), and Turner (*ex officio*). Also present, Ms.Dunn.

Mr. THORNBERRY. The subcommittee will come to order. This hearing of the Subcommittee on Cybersecurity, Science and Research and Development will take testimony today on Homeland Security Science and Technology: Preparing for the Future. It is the intention of the chairman and ranking member, Ms. Lofgren, that as many members as possible have a chance to ask questions. Therefore, we are going to ask that members strictly abide by the 5-minute rule and ask unanimous consent to waive oral opening statements beyond the chairman and ranking member, but allow all members to put a written opening statement into the record. And without objection, it is so ordered.

I want to welcome members, witnesses and guests to this hearing. This subcommittee is charged with oversight of several complex and important issues related to homeland security. During the nearly 2 years which Congress considered legislation to create the Department of Homeland Security, I became convinced that one of the keys to success for the new Department would be the ability to identify and research and develop and field quickly products and services that help make us safer. Getting this part right is very important, organizationally and operationally. And whether it is computer technology that allows us to integrate government databases or whether it is new detectors that help keep radiological material from coming into this country, technology is central to a safer America.

And yet we can not be satisfied with a government as usual approach where in the case of the things that are often discussed in this committee, it can take up to 20 years to field new technologies. We are facing an enemy that is fast, nimble and lethally aggressive, and we have got to be just as fast and just as aggressive, not

just in pursuing the enemy, but in pursuing new technologies that help keep us safer.

That is why I know the subcommittee is anxious to hear today how the new Department is doing to set up the Science and Technology Directorate. We are interested to see how the Department intends to identify existing technologies that we need and get them out into the field quickly. We are interested to see how the new Department intends to conduct research and development and set priorities in those areas. We are interested in how we can best ensure a productive cooperative relationship with the private sector, the academic community and government, because we are all going to have to work together if we are going to be successful. We are interested in whether the Homeland Security Act of 2002 needs to be changed in some way to help us get the job done.

And I will say that this subcommittee is interested in being a full partner with the Department and the administration because it is only with a new kind of legislative executive partnership that we will be as successful as we need to be. We have a lot of challenges ahead of us. But obviously, we have the ability to work together and overcome them. Before yielding, I want to thank the Armed Services Committee for allowing us to use their facilities here. I also want to thank Eric Fischer and his team from the Congressional Research Service, who have done a terrific job in helping us prepare for this hearing, but also have prepared some outstanding reports, which I would commend to all members.

Finally, I want to thank my partner on this subcommittee, Ms. Lofgren, for her help and her contributions in getting this subcommittee started as we are getting the full committee going. Ms. Lofgren brings a wealth of knowledge and expertise to these issues, as well as a cooperative spirit, and I certainly look forward to our continued work together and I would yield to her at this time.

PREPARED STATEMENT OF THE HONORABLE MAC THORNBERRY, CHAIRMAN, SUBCOMMITTEE ON CYBERSECURITY, SCIENCE, AND RESEARCH & DEVELOPMENT, SELECT COMMITTEE ON HOMELAND SECURITY

I want to welcome Members, our witness, and guests to this hearing conducted by the Subcommittee on Cybersecurity, Science, and Research and Development of the Select Committee on Homeland Security.

This Subcommittee is charged with oversight of several complex and important issues related to homeland security.

During the nearly two years that Congress considered legislation to create the Department of Homeland Security, I became convinced that one of the keys to success for the new Department would be the ability to identify, research, develop, and field products and services quickly. Getting this part right—organizationally and operationally—is very, very important.

Whether it is computer technology that allows government agencies to see the full range of information about a potential visitor to the United States or various sensors and detectors that help prevent weapons of mass destruction from being smuggled into the country, technology is central to a safer America.

Yet, to be successful, we cannot be satisfied with a standard, government "business as usual" approach. We must do better. We are facing an enemy that is fast, nimble, and lethally aggressive. We've got to be just as fast and just as aggressive, not just in pursuing this enemy, but in pursuing new technologies that will help keep our cities and towns more secure.

That's why the Subcommittee is anxious to hear how far along the new Department is in setting up the Science and Technology Directorate.

That's why we're interested to see how the Department intends to identify existing technologies that are needed for homeland security and then field them quickly.

That's why we're interested to see how the Department intends to conduct research and development in areas that are needed but do not presently exist.

We are also interested in how the Department intends to set priorities, rather than simply spread money around indiscriminately.

We're interested in how we can best ensure a productive, cooperative relationship among business, the academic community, and government because this challenge is going to require the best from all of us.

We're interested in whether the Homeland Security Act of 2002 that established the Department needs to be tweaked or changed in some way to make sure that the job gets done.

And we're interested in being full partners with the Department and the administration because it is only with a new kind of legislative-executive partnership that we will be as successful as we need to be in protecting our homeland.

We have enormous challenges before us—bureaucratic and political pressures among them. But together, we must overcome those challenges and quickly get tools that help protect and defend our homeland into the hands of those who need them.

Before I turn to our witness, I want to thank Eric Fischer and his team from the Congressional Research Service for helping to prepare for today's hearing.

I also want to thank my partner in this subcommittee, Ms. Lofgren, for her help and contribution to getting things going. She brings a wealth of knowledge and expertise to these issues, as well as a cooperative spirit, and I look forward to our continued work together.

Ms. LOFGREN. Thank you. Today is the first hearing for the Cybersecurity, Science and Research and Development Subject Committee. But before I make some brief comments on today's hearing, I want to take a minute to thank Chairman Mac Thornberry and his talented staff. I greatly appreciate your efforts to work in a bipartisan manner, and I look forward to cooperating with you in the coming months on the significant cybersecurity and technology challenges that our country faces. There is no shortage of issues that this subcommittee should address, and I am confident that we will be able to accomplish much together.

Today's hearing marks the second time that I have had the opportunity to hear Dr. McQueary testify in front of Congress in the past week. Dr. McQueary appeared before the House Science Committee last Wednesday, and the fact that he has testified before two different committees recently, underscores the importance that we in Congress place in the mission of the science and technology directorate and, of course, the Department of Homeland Security as a whole.

We face major challenges to secure our country. The Select Committee on Homeland Securities' oversight should be devoted to getting the new Department up and running as quickly and efficiently as possible. This subcommittee must also ensure that the issue of cybersecurity, science and research and development receive a proper level of attention within DHS itself.

I want to be assured that Dr. McQueary has the budget, staff, resources and most important, access to get the job done. Since our appointment to this subcommittee, Chairman Thornberry and I have spent much of our time studying and learning about the many complex issues involving cybersecurity, science and research and development. These issues are sometimes difficult to grasp and not as easy to comprehend as the threats to our borders and infrastructure. I believe it is important for this subcommittee to help inform the public by explaining the threats and vulnerabilities involved in cybersecurity. I hope that Dr. McQueary will spend some time today explaining these threats and vulnerabilities. If these issues are better understood, then we can better prepare and defend our

country and its citizens. I also would like to hear from you today on the Department's relationship with agencies like the National Science Foundation, the National Institute of Standards and Technology, and DARPA.

It is critical that DHS cooperates with these and other like agencies. The Department can gain valuable experience from each. However, I also think it is important that these agencies remain independent from DHS. I am concerned that the Department may drain these agencies of their resources, and I don't want to hear from the good people at NIST that all their best staff has been detailed to DHS.

Finally, I represent Silicon Valley, one of the most innovative places on earth. The people in the valley thrive on solving complex problems. Since my appointment, countless engineers, programmers, professors, researchers and high tech CEOs have approached me to express their interest in helping DHS with their mission. Some have innovative homeland security products. Others have theories on information systems protection, and some have seen, done academic studies on cybersecurity. All have valuable expertise to offer.

The problem that almost all encounter is they do not know whom to approach to pass on their experience and ideas, and I hope that Dr. McQueary will shed some light on the structure of the science and technology directorate. I want to know what office will handle inquiries from the private sector and academic community. Thank you again for appearing today. I look forward to working with you, Dr. McQueary, in the weeks and months to come and certainly, our very able Chairman Thornberry, and I yield back the balance of my time, Chairman.

Mr. THORNBERRY. I thank the gentlelady. And Dr. McQueary, let me welcome you. Let me explain just briefly that there are a variety of things going on at this time. Your colleague, Asa Hutchinson, is over in the Capitol giving a briefing to members and members are coming and going. I think there may also be a markup in the Judiciary Committee. I would yield to the gentleman from Texas, Mr. Smith, briefly for his personal explanation.

Mr. SMITH. Thank you Mr. Chairman. First of all, of course, thank you for convening such an important hearing. I don't know of a more important subject we can be considering. Also having served as the chairman of the Crime Terrorism Homeland Security Subcommittee, I have a special interest in cyber crime. Having said that, however, I do have a markup of the Judiciary Committee that is going on right now, so I want to explain to you and to our witness why I need to be leaving immediately. But I would ask you if it is at all possible to submit three questions that I have in writing to our witness and hope for a response in a reasonable amount of time.

Mr. THORNBERRY. We will absolutely do so. Without objection those questions will be submitted for the record and we will work with the folks at the Department to get an answer.

[The information follows:]

PREPARED STATEMENT THE HONORABLE ZOE LOFGREN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Today is the first meeting of the Cybersecurity, Science, and Research & Development Subcommittee. Before I make some brief comments on today's hearing, I want to take a minute to thank Chairman Mac Thornberry and his talented staff. I greatly appreciate it your efforts to work in a bipartisan manner, and I look forward to cooperating with you in the coming months on the significant cybersecurity and technology challenges that our country faces. There is no shortage of issues that this subcommittee should address, and I am confident that we will be able to accomplish much together.

Today's hearing marks the second time that I have had the opportunity to hear Dr. Charles McQueary testify in front of Congress in the past week. Dr. McQueary appeared before the House Science Committee last Wednesday. The fact that Dr. McQueary has testified before two different committees recently underlines the importance that we in Congress place in the mission of the Science and Technology Directorate, and of course, the Department of Homeland Security (DHS) as a whole.

We face major challenges in trying to secure our country. The Select Committee on Homeland Security's oversight should be devoted to getting the new Department up and running as quickly and efficiently as possible. This subcommittee must also insure that the issues of cybersecurity, science, and research & development receive a proper level of attention within DHS itself. I want to be assured that Dr. McQueary has the budget, staff resources, and most important, the access to get the job done.

Since our appointment to this subcommittee, Chairman Thornberry and I have spent much of our time studying and learning about the many complex issues involving cybersecurity, science, and research & development. These issues are difficult to grasp, and not as easy to comprehend as the threats to our boarders and infrastructure. I believe it is important for this subcommittee to help inform the public by explaining the threats and vulnerabilities involved in cybersecurity. I hope that Dr. McQueary will spend some time today explaining these threats and vulnerabilities. If these issues are better understood, then we can better prepare and defend our country and its citizens.

I also would like to hear from you today on the Department's relationship with agencies like the National Science Foundation (NSF), the National Institute of Standards and Technology NIST), and the Defense Advanced Research Projects Agency (DARPA). It is critical that DHS cooperate with these and other like agencies. The Department can gain valuable experience from each. However, I also think it is important that these agencies remain independent from DHS. I am concerned that the Department may drain these agencies of their resources. I do not want to hear from the good people at NIST that all of their best staff has been detailed to DHS.

Finally, I represent Silicon Valley, one of the most innovative places on Earth. People in the Valley thrive on solving complex problems. Since my appointment, countless engineers, programmers, professors, researchers and high tech CEO's have approached me to express their interest in helping DHS with their mission. Some have innovative homeland security products, others have theories on information system protection, and some have even done academic studies on cybersecurity. All have valuable expertise to offer. The problem that almost all encounter is that they do not know whom to approach to pass on their experience and ideas. I hope Dr. McQueary will shed some light on the structure of the Science and Technology Directorate. I want to know what office will handle inquiries from the private sector and academic community.

Thank you again for appearing today. I look forward to working with you in the weeks and months to come.

PREPARED STATEMENT OF THE HONORABLE SHEILA JACKSON-LEE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

Mr. Chairman and Mr. Ranking Member, I thank you for convening this important hearing today to continue our efforts to protect our homelands.

I look forward to hearing the testimony of our witness today. The Department of Homeland Security's Directorate of Science and Technology has a unique function. The Directorate is charged with developing and deploying cutting edge technologies and new capabilities so that the men and women responsible for protecting our homeland can do so most efficiently.

The development of new technologies to protect our homeland opens the door to possible violations of personal rights and invasions of privacy. I am particularly con-

cerned about the use of the internet to invade privacy in the name of conducting law enforcement investigations.

The Select Committee on Homeland Security's Subcommittee on Cybersecurity, Science, Research, and Development has the responsibility of ensuring that violations of personal privacies and rights do not occur while still giving law enforcement agents adequate discretion to do their jobs.

The Internet has become a cornerstone of our economy and information network. Our national infrastructure depends on maintaining the distribution of goods and services that are essential to the defense and economic security of the United States. To an ever increasing extent, this distribution is becoming dependent on the free use of the Internet. I am concerned that we will diminish the value of the Internet in our haste to protect the country against terrorist attacks.

In addition to the use of the Internet as a market place for goods and services, the Internet may be the most perfect embodiment of the American ideals of free speech, open communication, and the "marketplace of ideas" that has ever existed. As the Supreme Court has written, online "any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox."

Speakers and listeners with great and small resources have access to an almost unlimited amount of content and diversity of views. That marketplace of ideas is threatened when monopolies that control access to the Internet can also control the available speech.

Internet Service Providers control both the content and the services that their customers can receive, which gives them the power to shape the market place of commercial goods and of ideas. It concerns me that commercial organizations have such power, but I am even more concerned about the power that the government is capable of assuming in its efforts to ensure cybernet security against terrorists.

The United States has now reached the point where a total surveillance society has become a realistic possibility. Many people still do not grasp that Big Brother surveillance is no longer the stuff of books and movies. Given the capabilities of today's technology, the only thing protecting us from a full-fledged surveillance society are the legal and political institutions we have inherited as Americans. Unfortunately, the September 11 attacks have led some to embrace the fallacy that weakening the Constitution will strengthen America."

From government watch lists to secret wiretaps - Americans are unknowingly becoming targets of government surveillance. It is dangerous for a democracy that government power goes unchecked and for this reason it is imperative to maintain government accountability, no matter how frightened we become by the threat of terrorism.

I look forward to hearing Dr. McQueary's testimony to address these concerns.

PREPARED STATEMENT OF THE HONORABLE BOB ETHERIDGE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NORTH CAROLINA

Thank you, Chairman Thornberry and Ranking Member Lofgren, for holding this hearing. I would also like to welcome Dr. Charles McQueary who hails from the great state of North Carolina, although he does not have the privilege of living in the Second Congressional District.

The work of the Science and Technology Directorate of the Department of Homeland Security is critical in the protection of Americans both here and abroad. This group is responsible for research and development of technologies that will protect not only our nation's critical infrastructure, but more importantly, the products developed by this group, in conjunction with private contractors and other government agencies, will help supply and protect our first responders.

I understand that the Directorate's immediate priorities include developing and deploying systems to help protect the United States from illicit radiological, nuclear, biological and chemical agents, as well as high explosives. I am glad to see that the Directorate intends to work closely with private industry to identify appropriate and!or adaptable products that are on the shelf or in the development pipeline. Our country is blessed with entrepreneurs with great talent, good ideas and amazing ingenuity, and it is incumbent upon the federal government to utilize these resources.

America is also the home of some of the best research universities in the world, many of them in North Carolina. The professors, researchers and students at these world-class institutions are involved in cutting-edge research that have a broad array of applications for homeland security. It is critical that the Department of Homeland Security encourage and foster this research, as well as the education of the scientists, mathematicians and other technologists our country needs now and in the future to continue America's tradition of state-of-the-art research and development.

I also look to the Science and Technology Directorate to look beyond colleges and universities to promote science and math education for our children. In the 2001 Hart-Rudman report "Road Map for National Security: Imperative for Change," the authors state that the greatest threat to our country, second only to the detonation of a weapon of mass destruction, would be "a failure to manage properly science, technology and education for the common good over the next quarter century."

The Department of Homeland Security will have to balance response to current threats with long-range planning. Currently, one-third of all U.S. science and engineering doctoral degrees and 40 percent of PhDs in computer science go to foreign students. Studies have shown that American students sorely lag behind their counterparts in other nations in science and math education. Many students who do go on to college do not enter technology fields because they see it as "too hard," and the financial rewards do not seem to balance the time and effort it takes to get advanced degrees needed for top-level research positions.

The federal government must work with private industry and schools across the country to improve basic science and math education by providing teachers with the opportunities for advanced training in these fields, the proper equipment for labs and experiments, and time to teach. Gifted teachers prove every day that students can learn and come to love science and math. Our children are our future, and investment now in their educations will provide benefits for many years to come.

Secretary McQueary, thank you again for briefing our Subcommittee on the Science and Technology Directorate. I am sure that our questions and concerns will necessitate many repeat visits, and I look forward to working with you to determine the best products, methods and procedures for protecting our country.

Mr. THORNBERRY. Let me now recognize our witness, honorable Dr. Charles McQueary, Under Secretary for Science and Technology. Dr. McQueary has previously served as president of the business units for General Dynamics, AT&T and Lucent Technologies. Perhaps most impressively, he holds a Ph.D. in engineering mechanics and an M.S. in mechanical engineering from the University of Texas. And no further qualifications are necessary.

Dr. McQueary, thank you for being here and the floor is yours.

STATEMENT OF THE HONORABLE CHARLES McQUEARY, PH.D., UNDER SECRETARY FOR SCIENCE AND TECHNOLOGY, SCIENCE AND TECHNOLOGY DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY

Dr. MCQUEARY. Thank you, Mr. Chairman. Congresswoman Lofgren, distinguished members of the committee, it is a pleasure for me to be here today to discuss the Department of Homeland Security's Science and Technology Directorate. It is a great honor and a great responsibility to lead the science and technology efforts of this Directorate and the Department to meet the challenges of protecting our homeland and our way of life. 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 secure our homeland can perform their jobs more effectively and efficiently. They, as well as the American people, are my customers.

Our plans for fiscal year 2004 reflect this relationship and our desire is to provide capability to the field as rapidly as possible. The threats to our homeland are many. We must constantly monitor these threats and assess our vulnerabilities to them. We must develop new and improved capabilities to counter chemical, biological, radiological and nuclear, explosive, and cyber threats. And we must mitigate the effects of terrorist attacks should they occur. The Science and Technology Directorate's program 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.

This Directorate will support the mission needs of the Information Analysis and Infrastructure Protection Directorate, the Border and Transportation Security Directorate, the United States Coast Guard, the United States Secret Service, and the Emergency Preparedness and Response Directorate through coordinated and focused research and development programs. Through the initial planning process for the Science and Technology Directorate, we were guided by current and future threat assessments, by our current capability to respond to that threat, and by the priorities spelled out in the President's National Strategy for Homeland Security.

Thus, our key specific areas of emphasis are listed as follows: 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. Second item is to 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.

Third, provide state-of-the-art high-performance, low-cost-operating systems to detect and prevent illicit high explosive transit into and within the United States. Fourth, enhance the missions of the Department operational units through targeted research, development, test and evaluation, and systems engineering and development. Fifth, develop and provide capabilities for protecting cyber and other critical infrastructures. Sixth, develop capabilities to prevent new technology as a surprise by anticipating emerging threats. And finally, item Number 7, develop, coordinate, and implement technical standards for chemical, biological, radiological, and nuclear countermeasures.

We will implement our activities through focused portfolios that support our mission. These portfolios are as follows: biological countermeasures, chemical and high explosive countermeasures, radiological and nuclear countermeasures, critical infrastructure protection, threat and vulnerability testing and assessment, and the standards and State and local program. Through the Homeland Security Advanced Research Projects Agency, our directorate will explore cutting-edge approaches to addressing current and emerging threats. It is our estimate that at least $350 million of the overall requests will be carried out by a HSARPA in fiscal year 2004. Our strategy includes evaluation, prototyping and rapid deployment of available technologies to the field.

To do this, we will establish a technology clearinghouse and partnership with the Technology Support Working Group, which has performed a similar mission over the past several years with great success for the Departments of State and Defense. Through this partnership, we will encourage and support innovative solutions to enhance homeland security, and we will engage the private sector in rapid prototyping of homeland security technologies.

A knowledgeable workforce focused on Homeland Security is essential to our ability to address advancements in science and technology. Declining enrollments in specific academic fields such as radiochemistry is leading to a lack of workers in areas of science

and technology, important to America's efforts to protect the homeland. Therefore, we will establish fellowship programs at the graduate and post-graduate levels to encourage research activities in these areas, and thus develop the foundation America needs to sustain our technical advantage in the war against terrorism.

We will also establish university centers of excellence to provide an enduring and focused research capability to the Nation in this effort.

Mr. Chairman, thank you again for the opportunity to appear before this subcommittee. This concludes my prepared statement. With the committee's permission, I would like to request that my formal statement be submitted for the record.

Mr. THORNBERRY. Without objection.

PREPARED STATEMENT OF THE HON. DR. CHARLES E. MCQUEARY

Introduction

Good afternoon. Chairman Thornberry, Ranking Member Lofgren, and distinguished members of the subcommittee. It is a pleasure to be with you today to discuss the Department of Homeland Security's Science and Technology Directorate. It is a great honor and a great responsibility to lead the science and technology efforts of this Directorate and the Department to meet the challenges of protecting our homeland and our way of life.

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 secure our homeland can perform their jobs more effectively and efficiently—they are my customers. Our plans for fiscal year 2004 reflect this relationship and our desire to provide capability to the field as rapidly as is possible.

The threats to our homeland are many. We must constantly monitor these threats and assess our vulnerabilities to them; develop new or improved capabilities to counter chemical, biological, radiological, nuclear, explosive, and cyber threats; and mitigate the effects of terrorists attacks should they occur. The Science and Technology Directorate's program must also enhance all of the Department's missions, whether or not they are focused on the threat of terrorism.

Throughout the initial planning process for the S&T Directorate we have been guided by the Homeland Security Act, current threat assessments, our understanding of capabilities that exist today or that can be expected to appear in the near term, and, importantly, by the priorities spelled out in the President's National Strategy for Homeland Security.

Thus, our key specific areas of emphasis are to:

- 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.
- 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.
- 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.
- Enhance missions of all Department operational units through targeted research, development, test and evaluation (RDT&E), and systems engineering and development.
- Develop and provide capabilities for protecting cyber and other critical infrastructures.
- Develop capabilities to prevent new-technology as a surprise weapon by anticipating emerging threats.
- Develop, coordinate and implement technical standards for chemical, biological, radiological, and nuclear (CBRN) non-medical countermeasures.

Research, Development, Test and Evaluation Portfolio

We are requesting $803M in fiscal year 2004 to provide applied research, development, demonstrations, and testing of products and systems that address these key areas of emphasis. The Science and Technology Directorate will implement its activities through focused portfolios that address biological, chemical, radiological and

nuclear, and cyber threats; support the research and development needs of the operational units of the Department; and receive innovative input from private industry and academia as well as national and Federal laboratories. In particular, the Homeland Security Advanced Research Projects Agency (HSARPA) will have an essential role in meeting the goals and objectives of the Department and the Directorate across the range of the portfolios.

These portfolios and activities are described as follows:

Biological Countermeasures—Biological threats come in many forms. They can be toxins, viruses, or bacteria, distributed by airborne aerosols, or in food or water supplies, or in the case of contagious diseases, spread among infected people or animals. Timely detection and early initiation of prophylaxis and decontamination is the key to mitigating the consequences of any biological attack, should it occur. We are requesting $365M in fiscal year 2004 to:

- Develop and deploy a Biological Warning and Incident Characterization System (BWIC). BWIC will consist of three major elements: a nationwide bio-surveillance system that looks for early biological indicators of the exposure of people, animals and plants to biological agents; development of a public health surveillance system working through the Department of Health and Human Services and its Centers for Disease Control and Prevention's (CDC) public health surveillance system to detect early adverse health events in the population as a result of such agents; and environmental monitoring networks in selected cities that can detect the agent directly. S&T plans to work closely with the CDC in developing this seamless sentinel system. This activity will be available as a pilot in fiscal year 2004.
- Continue the National Biodefense Analysis and Countermeasures Center (NBACC), initiated in fiscal year 2003, as a key component in implementing the President's National Strategy for Homeland Security. The NBACC will leverage the expertise of America's cutting- edge medical and biotechnical infrastructure to focus on the biological agent threat, including performing risk assessments. It is an essential, new approach to integrating national resources for homeland security, supporting public health, and law enforcement. The analytical capabilities of the NBACC will be functional in fiscal year 2004, and closely coordinated with the National Institute of Health and the Food and Drug Administration.

Finally, the Plum Island Animal Disease Center is expected to be transferred from the Department of Agriculture to DHS in June 2003. We plan to work closely with USDA in areas of mutual concern in animal disease research and diagnostics.

Chemical Countermeasures—According to the National Research Council's Report Making the Nation Safer, "chemicals continue to be the weapon of choice for terrorist attacks. They are readily available and have the potential to inflict significant casualties." In fact, terrorist attacks on civilian populations with chemical warfare agents have already occurred. In the Aum Shrinrikyo attack on the Tokyo subway, casualties were limited only because the attackers did not use an effective agent dispersal method. Similarly, accidental releases of toxic industrial chemicals have demonstrated that materials relatively widely available in modern industrial societies can result in a large number of casualties.

Significant work on chemical defense in military situations has been conducted focusing on battlefield attacks using chemical warfare agents. However, major gaps exist regarding civilian defense, most notably in strategies for dealing with the broader spectrum of threats (e.g. toxic industrial materials); detection systems capable of continuous monitoring with very low false positive rates; deployed chemical defense systems; and a robust forensic capability. The Chemical Countermeasures portfolio is requesting $55M to address these shortcomings through a balanced mix of activities: 1) systems studies will be used to prioritize efforts amongst the many possible chemical threats and targets; 2) new detection and forensic technologies will be developed and demonstrated; 3) protective systems that integrate physical security, ultra-sensitive detection, information management, and consequence management strategies will be developed and piloted in selected high value facilities such as airports and subways; 4) the Science and Technology Directorate will work with the Information Analysis and Infrastructure Protection and Borders and Transportation Security Directorates to characterize and reduce the vulnerability posed by the large volumes of toxic industrial materials in use by the critical infrastructures, stored or transported within this nation; and 5) ensuring coordination with the CDC for public health response and management of detected events.

High Explosives—Detection of high explosives and mitigation is now a prime focus of the Transportation Security Administration (TSA). The current terrorist threat extends beyond air transport to all other modes of transportation and fixed facilities.

The Department of Homeland Security will build on TSA's R&D in this area to develop and deploy more effective explosives detectors that can address the broader threats. Development of reliable stand-off detection capability of large quantities of explosives, especially in vehicles, is particularly needed. For this purpose $1OM is requested in fiscal year 2004.

Radiological and Nuclear Countermeasures—Countering the threat of radiological or nuclear attack is one of the top priorities of the Department of Homeland Security and the Science and Technology Directorate. The Radiological and Nuclear Countermeasures portfolio is requesting $13 7M to address this threat through a comprehensive systems approach that emphasizes early detection; effective intervention capabilities at the Federal, state and local levels; development of mitigation technologies and science-based consequence management programs for use should an attack occur; and effective training at all levels of response. Concurrent efforts focused on deployment, evaluation and improvements to currently available technologies; a research and development program for advanced technologies and their continuous insertion into operational use; and the provision for an enduring science and technology base to address long-term challenges such as the detection of highly-enriched uranium and heavily shielded radioactive sources is used to address both today's threats and those of the future.

Threat and Vulnerabilitvg Testing and Assessment—The purpose of the Threat and Vulnerability, Testing and Assessment (TVTA) program is to create advanced modeling, and information and analysis capabilities that can be used by the organizations in the Department to fulfill their missions and objectives. One thrust of this program is to develop advanced computing, information, and assessment capabilities in support of threat and vulnerability analysis, detection, prevention and response. This portfolio also conducts extensive research and development activities in the area of cybersecurity, 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 TVTA program uses a strategy of multi-year investments that infuse new capabilities into the DHS mission directorates on a regular basis based on strategic five year road maps. A spiral development process ensures early use and feedback by intended users and operators of all technologies developed within the program. Successively, more complete and refined prototypes lead to operational pilots and fully operational systems for the Department organizations. $90M is requested in fiscal year 2004 to support this activity.

Critical Infrastructure Protection—Our national infrastructure provides the continual flow of goods and services that are essential to the defense and economic security of the United States. Many of these functions are so vital that major disruptions would cause severe consequences to the behavior and activities of our citizens. Our free society and the high quality of life that we value depend upon the reliable operation of the infrastructure. In addition, we must protect the lives of our citizens and key assets such as many national monuments and icons.

The Critical Infrastructure Protection (CIP) portfolio has three primary goals: (1) develop, implement, and evolve a rational approach for prioritizing CIP strategies and resource allocations using modeling, simulation, and analyses to assess vulnerabilities, consequences, and risks; (2) propose and evaluate protection, mitigation, response, and recovery strategies and options; and (3) provide real-time support to decision makers during crises and emergencies—$5M is requested in fiscal year 2004 for this activity, which also leverages work being done elsewhere in the Federal government and the Department of Homeland Security.

Standards/State and Local Programs—Standards should be applied to all elements of the homeland security infrastructure to ensure a robust capability to defend against and to respond to any crisis situation—whether it is the result of terrorism, natural causes, or a catastrophic accident. Organizing and integrating the efforts of the government and the private sector will enable the Department of Homeland Security to develop standards for equipment used for detection of materials that could be used in a terrorist attack. This will reduce the probability of a successful terrorist attack on the United States and facilitate development of a vital and enduring ability to respond to national emergencies.

The Standards/State & Local Program will provide consistent and verifiable measures of effectiveness of homeland security related equipment and systems in terms of basic functionality, appropriateness and adequacy for the task, interoperability, efficiency, and sustainability. The Science and Technology Directorate will facilitate the development of guidelines in conjunction with both users and developers. The guidelines will encompass user needs and operating conditions, as well as the capabilities and the limitations of the technologies. The Standards/State and Local Program will develop, in collaboration with operational end-users, performance measures, testing protocols, certification methods, and a reassessment process appro-

priate to each threat countermeasure and for the integrated system. The Standards/ State and Local Program will address all elements of the homeland security mission including equipment, information, analyses, personnel, and systems. Special emphasis will be placed on soliciting input from the actual users in the state and local response communities, and on providing effective methods for communicating information back to these agencies.

Major program objectives include working with the private sector to establish a network of homeland security certification laboratories. This will provide a consistent level of assurance in the effectiveness of detection and other operational equipment. Consistent standards for training and certification of personnel will also be developed. The program will continue to broaden the suite of technical standards for various forms of equipment and systems and will provide protocols and standard data collection formats for test and evaluation projects undertaken by the Science and Technology Directorate. $25M is requested in fiscal year 2004 to support this important effort.

Support to Department of Homeland Security Components—The Science and Technology Directorate has the responsibility to provide Federal, state and local operational end-users with the technology and capabilities to protect the United States homeland from catastrophic terrorist attacks and enhance their capabilities for conducting their conventional missions. An essential component of this responsibility is to coordinate and collaborate with the other components of the Department to assist and enhance their technical capabilities through integrated research and development activities. The integration of the Science and Technology Directorate research and development efforts with the Information Analysis and Infrastructure Protection Directorate is specifically described in the Threat and Vulnerability, Testing and Assessment, and the Critical Infrastructure Protection portfolios. In addition, the Science and Technology Directorate will support the mission needs of the Border and Transportation Security Directorate, the United States Coast Guard, the United States Secret Service and the Emergency Preparedness and Response Directorate through coordinated and focused research and development programs. Research and development in potentially high payoff technologies will be emphasized. $55M is requested in fiscal year 2004 for this purpose.

Rapid Prototyping Program—Significant capabilities exist in private industry for the rapid development and prototyping of technologies in support of the homeland security mission. A mechanism to quickly and easily access the capabilities of private industry will allow the Department of Homeland Security to more effectively fulfill its mission requirements. The Science and Technology Directorate will establish a partnership with the Technical Support Working Group (TSWG) to provide the Department with a technology clearinghouse to encourage and support innovative solutions to enhance homeland security and to engage the private sector in rapid prototyping of homeland security technologies. $30M is requested in fiscal year 2004 to solicit from the private sector near-term capability that can be rapidly prototyped and fielded.

Homeland Security Fellowship Programs Programs—Advancements in science and technology have the potential to change or increase the threats to our security; these advancements also improve our ability to thwart these emerging threats, A knowledgeable workforce focused on homeland security is essential to our ability to address advancements in science and technology.

The vast scope of the science and technology needed to address homeland security coupled with declining enrollments in specific areas such as nuclear science and technology, and radiochemistry are leading to a lack of qualified applicants for relevant research and development. This program requests $10M to support strategic partnerships with the academic community to provide support for qualified students and faculty.

Emering Threats—Advancements in science and technology have the potential to change or increase the threats to our security. These advancements also improve our ability to thwart these emerging threats.

The Emerging Threats program will support the exploration of innovative, cross-cutting, out-of- the box approaches for anticipating and responding to new and emerging threats. It will also establish and support studies and analyses to be conducted by the new Homeland Security Institute. $22M is requested in fiscal year 2004 for this purpose.

The scope of the work to be conducted by this budget is broad but focused on the areas that improve our capabilities to thwart terrorist attacks by early detection and identification of the threat, effective protection and intervention technologies, mitigation of potential consequences should an attack occur, and a robust forensics and attribution capability. Our strategy includes early deployment of off-the-shelf technologies to provide initial defensive capability and near- term utilization of

emerging technologies to counter today's terrorist threats and the development of new capabilities to thwart future and emerging threats. A key part of our efforts will be conducted through the Homeland Security Advanced Research Projects Agency to engage industry, academia, government, and other sectors in innovative research and development to meet operational needs. Although I have described the budget request along product lines, such as biological and chemical countermeasures, it is our estimate that at least $350M of the overall request will be carried out by HSARPA in fiscal year 2004.

Mr. Chairman and members of the subcommittee, this concludes my prepared statement. I would be pleased to address any questions.

MCQUEARY. And I would now be pleased to answer any questions that you might have for me.

Mr. THORNBERRY. Thank you. I will reserve my questions towards the end and recognize the ranking member, Ms. Lofgren.

Ms. LOFGREN. Thank you, Mr. Chairman. And thank you, Doctor. I assume, from your testimony, that the technology clearinghouse, or partnership, would be the point of contact for individuals who have technology that they want to make known to you. I am wondering, and I think the chairman has had the same experience I have had, and I think all the members have had. I mean, there are a lot of people with good ideas and some of them aren't very good as well. There are people who are vendors and there is nothing wrong with that, but it is certainly not something that the committee wants to deal with.

We want to make sure that vendors are dealt with in an appropriate fashion administratively, but that good ideas have an opportunity to be heard because there are some very smart and innovative things that are out there. Can you tell us, with some detail, how people with ideas or products may interface with you specifically so that we can deal with these individuals in an appropriate manner?

Dr. MCQUEARY. I would be happy to do that. As you may recognize, we are just building the Science and Technology Directorate, and we are about 50 people at the present time and continuing to grow. And so our ability to be able to respond to all of the inputs we get has been limited from the standpoint of having face-to-face contact. So with that as the backdrop, we have really three methods that are available to us.

One, we have enlisted the Technical Support Working Group, from which we have recently issued a broad agency announcement to indicate areas that we have interest in, and we will also use that same organization to review for us and make recommendations on an e-mail site that we have. It is science.technology@dhs.gov, which, at the present time, I have, I would say, about 500 inputs that have come in from various industry sources. So those two areas. And then—when we see things that look like they might have near-term applicability we are actually inviting people in to meet with them to hear what kinds of things that might be of interest.

So it is really three methods that we have. And my objective is to get the point where we can respond in a very respectful and rapid way to the inputs we are getting, because I am finding there are an enormous number of ideas out in America that people have to offer for us, and what we need to do is be in a position to evaluate those.

Ms. LOFGREN. On a similar vein, there are certainly, you know, people with a product to sell are trying to sell a product and that may be good or bad depending on how good a product it is. The academic community has a different focus obviously. And I am aware, and I am sure other committee members are aware that there are some incredible talent out in our academic communities, and that is a lot of transportation to and fro between defense agencies and academia as well. Certainly, in California we have a wealth of information both at Berkley and at Stanford, and I am wondering if you can give us some insight on how we might best incorporate the wealth of talent information ideas that we find at such academic institutions with what you are doing in a way that would be most productive.

Dr. MCQUEARY. Well, first of all, if you know of something specifically, we would certainly encourage you to either contact us directly, have your staff contact us, or have someone from the organization contact us too using the methods that I described earlier, because we are anxious to hear about as many things as we can. I personally am trying to get out and to see and listen to as many different things as I can. Obviously my ability to be able to do that every day is not possible. And with our relatively small staff, we are having it is a challenge to be able to get the people out on the road to listen to the many different things. But universities are extremely important to us and will be an important part of our program as we go forward and we certainly expect to find cutting-edge research in the university.

We expect we will find instances where private industry and universities partner in order to create a broader capability to bring things to us. And so certainly, universities are going to be a key issue and, of course, we are going to identify some number of centers of excellence that will be in universities as a part of our overall program.

Ms. LOFGREN. Perhaps the committee could be of assistance to you, as we—the chairman and I have talked about our work plan through the year and even have thought about going out into the country and maybe we can collaborate, the three of us, on how to bring all of those talents together.

Dr. MCQUEARY. I would welcome the opportunity to discuss it in more detail with you.

Ms. LOFGREN. Last week, Chairman Boehlert asked if you could provide him with a list of people and dollars working on cybersecurity nwithin DHS. Have you had a chance to do that yet.

Dr. MCQUEARY. No, we have not. We have not completed that yet. But we will provide that as we indicated.

Ms. LOFGREN. I wonder if this committee could also get a copy of that.

Dr. MCQUEARY. Absolutely. We would be happy to do that.

Ms. LOFGREN. Thank you very much. Also last week, we asked if we could get a copy of the memorandum of understanding signed on May 19 between DHS and the Department of Commerce, specifically with NIST. Has the MOU been signed yet?

Dr. MCQUEARY. No, it actually has not been signed. We ran into scheduling difficulty and I expect to meet with Secretary Phil Bond tomorrow to accomplish that. That is the current plan. One never

knows when the schedule may have to be changed again, but that's our current plan.

Ms. LOFGREN. Again, perhaps this committee could also get a copy of this MOU.

Dr. MCQUEARY. Absolutely. Anything we have is available to you.

Ms. LOFGREN. Also, last week, we had a discussion—brief discussion of the—what is necessary to provide an analysis of biometric standards. And I see actually since the chairman's being very kind, my time is up and we probably will have time for a second round. I am going to reserve that question and set an example for all of us to stay within our 5 minutes.

Mr. THORNBERRY. The Chair thanks the gentlelady, and it is my intention to have another round of questions, particularly if folks are as good as the ranking member in observing the clock. The Chair would yield at this time to the vice chairman of the subcommittee, the gentleman from Texas, Mr. Sessions.

Mr. SESSIONS. I thank the chairman very much, and also greatly respect and appreciate the questions that have been asked by the ranking member.

Dr. McQueary, welcome. We are delighted that you are here today. As you can tell you have an eager group of members in front of you who are really after information from you to know how we should proceed. Obviously, I believe that the road map that you have given us today is not only well presented and well prepared, but gives us an idea of the measures that you have before you.

The first question I would have to you is as related to page 3, where you go through the seven pieces or piece parts, things that you are interested in doing. Where did these pieces—were they handled by some portion of government before you came into this job? Is someone else—had they developed these? It was somewhere, or was this something that you believe that the government is taking up for the first time?

Dr. MCQUEARY. If you could guide me, which page, what are you referring to?

Mr. SESSIONS. Page 3.

Dr. MCQUEARY. Of my oral remarks, or—

Mr. SESSIONS. Yes, sir. It would be in your oral remarks. For instance number one is develop and employ state of the art—

Dr. MCQUEARY. Oh, yes.

Mr. SESSIONS. Those things, did those—did you come up with those yourself, or had work been underway in some other part of the government and then you had to go in and extract that?

Dr. MCQUEARY. Well, if you go back to the President's National Strategy on Homeland Security, you will find that each and every one of those are listed as key priorities in the National Strategy. So we have taken that as explicit guidance of our work package. We have also reviewed it in areas to see whether it should be supplemented, and I would say that at this point, not only I but also the team who has been working on this are very comfortable with those seven items as being the key priorities for us.

Mr. SESSIONS. I am also. So include me in that list of people.

Dr. MCQUEARY. All right. Thank you.

Mr. SESSIONS. What my question is, sir, is had someone in this government been working on any of these products before you list-

ed them where there would be prior work that could be—had been done to where you would review, or at least take up where that had come? Because it seems like this will be, obviously, your function. Are you picking up the pieces of any of these from some work that had previously been done?

Dr. MCQUEARY. Yes. In fact, many of those items were already being investigated by the Department of Energy and that was transferred to us as a part of the overall restructuring to form the Department of Homeland Security. So most of those items that are listed there, and I could be—if you would like me to be—I would be happy to provide you with explicit ones.

Mr. SESSIONS. No. I am very happy—what you are saying is that some of this work had been going on. Did you get those people with them, too?

Dr. MCQUEARY. We did not—we received six people out of DOE, and in the case of work that's being done at the national labs, of course those people are available to us. But we did not get more than the six from DOE in terms of program managers and people who run the programs.

Mr. SESSIONS. These items that are listed here, come—and I think are listed properly, and I agreed with them, but they come at a high priority to this Congress and certainly the American public at this time. Can you talk with me about the rapid prototyping program and how quickly you believe that they will be to a point to where you are satisfied that they are producing not only the processes to evaluate these items, but to move them forward to where they become readily available to us? Would you mind spending just a minute and talking about that because that is going to decide, I believe, our success or failure in the immediate future. And your time table as to an evaluation there would help this committee.

Dr. MCQUEARY. If I could back up just a little from that question and provide a little bit more detail for you. Our primary focus today, if you will, and for the next several days and short number of months is to investigate what kinds of things already exist out in America today that we believe could be brought to the test stage where we could go into the field and try these things, and then initiate a development program and subsequent manufacture if that seems to be productive.

Now, I believe that you have—the question you have asked, I am interpreting that to be a little bit later in the process in which we have got, we have had an idea. We develop a prototype and we are not quite sure what to do. My experience in industry is that it is very important if you have a prototype you must go into a full-scale development within a short time frame, and also, in order to be able to effectively transfer whatever the product might be into manufacturing, if you expect to be able to get it in a timely fashion and at a cost, you can afford and get it on a schedule that—and be able to have it perform the way you want it to perform. So—

Mr. SESSIONS. Good. I completely agree with that. I am just going to make one additional comment, and then I am going to yield my time. It is my hope that we can as rapidly as possible, and is seems like it fits your philosophy, to determine as quickly as possible what is out there, how it might be used, quickly deployed.

And as long as we get something that's leading edge, I hope we don't have to be perfect with it.

Dr. MCQUEARY. I am believe the 95 percent quickly, is much better than 99 percent if it takes forever.

Mr. SESSIONS. Right. And so I am very hopeful that you will find that this rapid prototyping program lives up to its name. And I will be intensely interested in seeing the success of that. And I want to thank you for being here today. I yield back, chairman.

Dr. MCQUEARY. Thank you.

Mr. THORNBERRY. I thank the gentleman. And I think he is exactly right. The Chair yields to the gentleman from North Carolina, Mr. Etheridge.

Mr. ETHERIDGE. Thank you, Mr. Chairman. And let me welcome you again also and thank you. I want to ask one question, a little bit off of cybersecurity, but it's important. You visited, I think, in the last couple of weeks, with a number of the folks in universities in North Carolina. And one of the individuals, Dr. Barker, I believe, who is the director of Textile Production and Comfort Center, raised an issue about the need for consistent standards for first responder equipment. Could you sort of summarize where we are with that? You had indicated that we were going to be working with NIST to get a memorandum of understanding, so we would have a consistent standard across as we spent money on that very quickly. Can you sort of give us some indication of where we are?

Dr. MCQUEARY. Well, yes. As I indicated earlier, we expect to sign a memorandum of understanding with NIST tomorrow, assuming things come as we think they are. We have already issued the draft standards for radiological devices because those are important ones, and we would expect and we are doing that, by the way, in concert with support from NIST, as well as the American National Standards Institute, too, as well as some other standards agency. And so that is our approach. And we will continue that as being a long-term effort. We have, I believe, $15 million program in fiscal year 2003, and 25 recommended for fiscal year 2004 to make sure that we do continue that effort. It is very important.

Mr. ETHERIDGE. Great. Thank you, sir. Last week when you testified before the House Science Committee, you talked about the need for increased spending on cybersecurity and I think this committee feels strongly about that. Yesterday, Secretary Ridge indicated that more than 80 percent of the Nation's critical information infrastructure is in private hands. Now, that being true, let me just ask several questions and I'll try to keep them together. In addition to the Department of Homeland Security, how many Federal agencies are currently involved with assessing vulnerabilities and recommending solutions to the Nation's cybersecurity infrastructure?

Dr. MCQUEARY. The ones that I am most familiar with are the group that testified last week. DARPA has some work going on in that area, and NIST has work going on, as well as the National Science Foundation. And of course ourselves, with our emphasis being in the infrastructure, Information Analysis, and Infrastructure Protection Directorate with the strong scientific support from the Science and Technology Directorate.

Mr. ETHERIDGE. I guess my question to follow that then, the agency, you said you are working together. Are they cooperating in

a way that will further this research and development that we so badly need to do?

Dr. MCQUEARY. I believe so, sir. In fact, one of the things that I have found in doing this job is that the cooperation seems to abound when we talk about Homeland Security. There is a spirit of we need to be working together in order to do this major job that we all have to work in.

Mr. ETHERIDGE. And that invariably leads to the next question on overlap. I know it is early in the game. But I do hope that as you move along, that you will make every effort possible, that they won't have overlap, because obviously that is not the best use of resources when we have limited resources.

Dr. MCQUEARY. I completely agree with you, and I believe one of the major responsibilities I have is to make sure that we do not have overlap, not only in that area, but in other areas too. And that is why we are interested in finding out what is going on outside of Department of Homeland Security.

Mr. ETHERIDGE. Good. Now having come from the private sector, you will appreciate the next question I am going to ask, because it is one that many times people in the private sector and the public sector find a bit sensitive. And I think, given our charge and our challenge it should be asked and we need to deal with it. What role should the Federal Government play in ensuring that the private companies protect these critical information infrastructures that are so critical not only to them, but to the security of the American people?

Dr. MCQUEARY. Well, this is my view that the government can provide standards recommendation guidance, but I firmly believe, having come out of the private sector, that it is the individual company's responsibility in order to have a secure system for handling information. Quite frankly, I believe that those companies that rise to the occasion and do it well can find themselves at a competitive advantage over those who do not.

Mr. ETHERIDGE. And that will lead to one additional question, because in the 2001 Hart-Rudman report, the road map to national security imperatives for change, one of the critical issues that was pointed out in that was the failure to manage properly science technology and education for the common good over the next quarter of a century. It could be a very destructive issue for this country and our ability to compete and protect the homeland.

That being said, the Department of Homeland Security will have to balance the responses of the current threat with long-term planning. That is always the case, but it is going to be a critical piece. Currently, one-third of the U.S. science and engineering doctoral degrees and 40 percent of the Ph.D.'s in computer science are going to foreign students, many of whom are leaving this country. I hope there is some planning down the road and that this Department will get involved as well as others to help us deal with this issue. I see this as a real long-term challenge.

Dr. MCQUEARY. I agree with you, and that was one of the motivating factors in our deciding that we wanted to provide scholarships and fellowships from Homeland Security to get people focused on problems that are relevant to the mission that we have.

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

Mr. THORNBERRY. Thank the gentleman. The Chair yields to the gentleman from Georgia, Mr. Linder.

Mr. LINDER. Thank you, Mr. Chairman. I just have a couple of questions. How much are you using the CDC and how are you using them?

Dr. MCQUEARY. How much are we using the CDC?

Mr. LINDER. And how are you using them?

Dr. MCQUEARY. One of the key areas in our relationship with CDC is in the development of software programs that can give early indications of whether biological events might have taken place. And they have done some very good work on that, and we expect to continue to work with them to improve that. I think that's an area that we will certainly want to engage ourselves in extensively because I think it's really important, particularly in the biological area, to be able to have good information, be able to decide what do, and react quickly—more so perhaps than in any other of the other threats we have.

Mr. LINDER. Do you see them in anything other than biological?

Dr. MCQUEARY. That has been the primary—when I say "biological," I include in that illnesses, sicknesses and so forth. Maybe I didn't use the proper terminology, but that's what I mean.

Mr. LINDER. One of the reasons they have been so successful is they have understood their mission was an informational one. They put the scientists together and got the correct scientific information and made it available to other government local and State governments and they have had a huge success and I hope you will think about the value of sharing information. My personal view is that Homeland Security ought to be more informational than programmatic. Although there would be some of both there. But you are going to have to share information with first responders across the country, and get the best information and share it. The CDC has had a huge success in doing just that. It is a good model. Thank you, Mr. Chairman.

Mr. THORNBERRY. Thank you. I thank the gentleman. The Chair recognizes the gentlelady, Ms. Christensen.

Mrs. CHRISTENSEN. Thank you, Mr. Chairman and welcome Dr. McQueary.

Dr. MCQUEARY. Thank you.

Mrs. CHRISTENSEN. I will start out with two questions. In your testimony, you said the Science and Technology Directorate will implement it's activities through focus portfolios that address biological chemical, radiological et cetera and support research and development needs of operational units. The Department receives the innovative input from private industry and academia, as well as national and Federal laboratories. Mine is not a—my question is not related to cybersecurity either. We have had two hearings on Project Bioscience. And I wonder if you could tell me how your office relates to that, how you interact on the Project Bioscience, which has come before us and asked for the mandatory permanent funding and certain, support for certain programs that they want to implement that seem to be included in what I just read.

Dr. MCQUEARY. I would say at this point, our interaction with people of bioscience has been somewhat limited, just because we have only been in existence for a little over 2 months. But certainly we would expect to be engaged in the scientific discussions about what items should be considered under the bioscience guidance that has been proposed or that is bioscience. I guess we are still waiting for the final bill to be passed. But we would be a participant in that. I really could not go into any detail, because I simply don't know today how to answer your question in more specific detail than that.

Mrs. CHRISTENSEN. Well, in your role as the Under Secretary for Science and Technology, when projects like these are being developed, shouldn't they be developed in conjunction with your office?

Dr. MCQUEARY. Well, in this particular case, for bioscience the leadership role, as specified in the development in the bill that created Homeland Security, left the scientific work, if you will, largely with Health and Human Services. In fact, the budget for the work is included there. So we are in more of a support role to help make sure that from Homeland Security perspective that what goes on there is what is needed.

Mrs. CHRISTENSEN. OK. I wanted to ask a question about the university centers. Homeland Security Act requires the creation of one or more university-based centers for Homeland Security. How many centers do you expect to establish? How will you decide where to establish them? And I am particularly interested in the minority serving institutions and what outreach will be made to ensure that they participate and that their research infrastructure is at a level to allow them to participate.

Dr. MCQUEARY. The approach we—first of all we have not decided how many centers of excellence that we should have at this point. I am sure that we will have more than one, though. We have engaged already in discussions with the American Association of Universities, National Science Foundation, and the American Association for the Advancement of Science. Most of these, all of these groups represent affiliations, university membership in some form, and so we are asking for inputs as to whom those groups feel would be the most qualified universities to be considered to be the centers of excellence.

On the issue of minority colleges, you may, if you read my bio, you know that I was on the board of trustees for a historically black college, North Carolina A&T University, so I am intimately familiar with the value that such an institution can bring to the roles that we have to do here. And certainly, we will make sure, I can assure you that I will make sure that we will give due consideration to all schools as we look at where these centers of excellence should be.

Mrs. CHRISTENSEN. And Dr. McQueary, since this is a new—the Department is new, the times of research that we will be looking to do is relatively new, or building on some old research for a new purpose, would we anticipate that there would be funding to assist universities that may not have the capacity now to be able to have the capacity to be a centers of excellence, such as the HBCUs?

Dr. MCQUEARY. I have not had a discussion with anyone about that subject. But it is certainly one worthy of us considering, and,

if I could, if you pose a question, maybe I could offer you an answer after I have had a chance to think it through carefully, because it is an important question.

Mrs. CHRISTENSEN. Thank you. Thank you, Mr. Chairman.

Mr. THORNBERRY. I thank the gentlelady. The Chair yields to the gentleman from Pennsylvania, Mr. Weldon.

Mr. WELDON. I thank the chairman. Dr. McQueary, thank you for being here. I am going to run through some issues. You may not be able to answer them today. But I would like you to get back to us. A few years ago, 5 years ago we had an initiative underway called the MEDEA Project. Are you familiar with that?

Dr. MCQUEARY. No, sir, I am not.

Mr. WELDON. The MEDEA Project was designed by the Intelligence Community and our Defense Agency to allow a selected number of scientists around the country to get access to classified technology to assist us in both Homeland Security and in threats that were emerging. One of the initiatives that came out of that was called FIRESAT, where we took $14 million that I got plussed up as the chairman of the Defense R&D Committee to use our overhead satellites to detect forest and wildlands fires. That system was developed. It was a multi-agency function. The software was completed. There was a disagreement over who would fund it and who would operate it, and today the software sits in boxes in Crystal City, Virginia.

So while America burns and while forest fires eat up hundreds of billions of dollars a year, for this country and impose a significant homeland security threat for lack of $5 million to put the program back into place, that program is sitting in boxes. And I put Secretary Ridge on notice yesterday, he is a good friend of mine. We are going to hold the agency accountable this year.

Last year, Joe Albaugh convinced me to put language in the defense bill to move the program from NOAA to FEMA. I did that. And FEMA has jurisdiction. FEMA now says they can't fund it until 2005 or 2006. That's unacceptable, so I would urge you to use your office. This is not your fault. It is a problem you have inherited but it is a science and technology activity that could directly benefit the Homeland Security this year. Before the forest fire season occurs again, please use your good influence to assist us in that. And also, look at the possibility of doing similar type of things with the use of technology, primarily coming from DOD resources in the future.

As you probably know, I think communication is our biggest challenge domestically. We still do not have a domestic integrated communication system. There have been some cutting technology, like Raytheon has developed to give you a localized unit that you can pre-program in up to 14 separate frequencies at the site to give us that integration of high and low band digital and so forth. We need to expedite short-term solutions for our first responders, but have the long-term objective of creating a national integrated communication system, and with your background from Lucent and from Bell Labs, you know the problem here very well, the middle ware problem.

But it needs to be our top priority. Along with that, we need you to help convince Secretary Ridge that he has got to stand up and

mandate that we set aside frequency spectrum allocation for public safety. That's currently a big issue. APCO has made it one of there top priority agenda items. Jane Harman and I have introduced a bill to do that and we would really appreciate and use the support of the Agency to set aside that frequency.

Tech transfer. We are doing a terrible job in the military of transferring technology for the first responder. It is a disaster. And I say it as the vice chairman of our Defense Committee and former chairman of Defense R&D. I have been on most of our disasters in the country. And the lack of transferring existing technology is absolutely disgraceful. I will give you a case in point. A pet peeve of mine is that we develop GPS capability for use of our troops in the battlefield to know where they are. We have also developed sensor technology, and transmission technology for an undergarment that a soldier can wear that can not only tell you where the soldier is, but their vital signs. Their pulse, their breathing rate. That same technology needs to be made available immediately to the one million volunteers and paid firefighters and paramedics and police officers nationwide.

If we had had that technology up in Boston we wouldn't have lost six firefighters who got lost in the warehouse when their air supply ran out and no one knew where they were. So we have got to do a better job. And I think you can help from your position at pushing the Pentagon to get more of that technology out the door quicker. We spend $40 billion a year on technology for the military. That technology, when developed, should immediately be applied where applicable to the first responder. In the case of cybersecurity, two issues. Both involving education. I think the focus has got to be away from training young people how to use computers, to what I call information dominance, information security.

Purdue developed the first graduate degree program followed by the Navy post graduate school. I think we have got to do a more aggressive job in convincing universities to develop graduate level and post doctoral programs in information dominance.

In fact, to go beyond that. In the military and defense budget, we are looking at creating a cyber core. We would actually create a position like we do when we were short medical officers to run young students through undergrad and graduate programs, commissioning them as second lieutenants, just like we did with our doctors when we were short doctors so that we create a whole new generation of young officers that serve the military for up to 5 years, give us that core technology competence that we need and then allow them to go work for the private sector and maintaining the information security and dominance so vital for our private corporations and other entities.

So those are a few of my thoughts. And the final one, I am out of time, but I will put it on the record, is EMP. We don't hear much about. Most people don't even know what electromagnetic pulse is. You know what it is? It is perhaps the largest and most severe threat to our use of information technology, and along with the threat of directed energy, we need to have a whole focus on that. And so I would ask you to get back to us on what are you doing with the threat of EMP.

We have an EMP commission right now that's working for DOD, but also the whole threat posed by directed energy weapons. Thank you.

Dr. MCQUEARY. Yes, sir.

Mr. THORNBERRY. The Chair recognizes the gentleman from New Jersey, Mr. Andrews.

Mr. ANDREWS. Thank you, Mr. Chairman. I appreciate the witness's testimony. I apologize for not being personally present, but I did have a chance to read it. Doctor, I want to ask you a question about how we best assure the cyber defenses of critical infrastructure in the nongovernmental sector in the utility companies, banks, health care institutions and so forth. First of all, would you agree with the assertion that cyber defenses generally speaking in the private sector are not as high as they technologically could be.

Dr. MCQUEARY. I would agree with that statement yes, without—that's obviously a very general answer.

Mr. ANDREWS. It is. And let me add parenthetically I do not mean that as a critical statement of the private sector. The private sector's responsibility is to protect its proprietary and commercial interests. If it extends beyond that point, it is frankly doing a disservice to the owners or shareholders of the venture. I don't mean to be critical. It seems to me that—would you also agree with the statement that some of the private sector critical infrastructure institutions in cyberspace are very critical indeed, that they are—they deal with our power grid, with our health care system and so forth. Would you agree with that.

Dr. MCQUEARY. I do agree with that.

Mr. ANDREWS. In thinking about this problem, it strikes me that there are four ways that we could approach it. The first is to kind of let the market run its course and let the private industry do what it will do, but no more. The second would be to mandate that private industry harden their defenses on a continuous basis to the highest level, which I think would be an unfair imposition of a public responsibility on private sector institutions. The third option would be to in effect nationalize these institutions to, to have the government take over the power grid, the government take over the 911 system in every way. I think this would be antithetical to our way of doing things and it is a proposal I would never embrace.

And the fourth way would be to find some appropriate way to subsidize the hardening of cyber defenses to the extent that the market will not harden those defenses, but no more than that, so that we are providing an appropriate level of public subsidy or incentive to raise that cyber barrier to its highest level but not to do so in such a way that we are having the taxpayers pay for something that the private concerns themselves might pay for. My question to you is, have I left out any alternatives? And if so, what are they? And the second, as a general strategy among those four choices, what would you suggest that we follow to try to harden those critical infrastructure cyber defenses.

Dr. MCQUEARY. Well, you asked two questions. Let me try both. I—just sitting here, as you are talking, I couldn't think of another, but I also would like to request the time to go back and talk to the people who are more intelligent than I am on this subject.

Mr. ANDREWS. Well, you are certainly more intelligent than me. So I would welcome that opportunity.

Dr. MCQUEARY. And trying to choose one as I am sitting here, I don't think it is appropriate as a scientist to make such a critical choice as we sit here talking about this in this form. But I would be happy to consider it and offer you my opinion based upon a considered thought process.

Mr. ANDREWS. I would certainly welcome that and I would welcome the chance to be briefed on that and share it with the rest of the committee as well. I raise this issue because it is my observation as an amateur in this area that the places in cybersecurity where we are most vulnerable are the places typically not controlled by the Department of Defense or by the Federal Government. Thank goodness, because we are a society that's not nationalistic in that way. But, it is—the problem here is that we are dealing with cyber defense in the private sector as a commercial venture. But it is a national security problem. And if someone wanted to attack us by shutting down the power grid, they would be attacking the systems of the utility companies and other private entities.

If someone wanted to create chaos by diverting 911 calls away from dispatchers, they would be attacking the systems of telecommunications companies and local governments where we are most vulnerable, we are least able to control by Federal law. So we have to find some way that does not exercise control and therefore substitutes, you know, this institution for the ones that do a much better job than we would.

But we still have to find a way to do it. I mean, my experience in this has been that in the military side, we have made great strides in the last few years since operation eligible receiver and some of the other exercises of the late 1990's, where DOD systems are hardened and they are being hardened on a continuous basis. But the critical infrastructure has nothing to do with that. And I think one of our real challenges and one the Department's challenges is to figure out a way to do that, to push those walls out further without imposing an unfair burden on private industry, but by getting the job done. I would welcome your thoughts and the Department's input. Thank you.

Dr. MCQUEARY. Thank you.

Mr. THORNBERRY. I thank the gentleman for his thoughtful questions and contribution and I would just chime in briefly, Dr. McQueary, that I think this is obviously a key subject of interest to this subject committee, and we want to work with you as well as the IP folks at the Department on the best approach. The gentleman from New Jersey has obviously put lots of thought and has lots to offer in this area. The subcommittee is very pleased that the Vice Chair of the full committee is with us, and the Chair would yield to the gentlelady from Washington for questions that she might want to ask.

Ms. DUNN. I thank you very much, Mr. Chairman. Welcome, Dr. McQueary. It is great to have you here and to get an update on how busy you have been since you took over this operation.

Dr. MCQUEARY. Thank you.

Ms. DUNN. I represent a district in Washington State, a district that is very close to a major deepwater port, the third largest port in the United States. And also has about 120 miles of maritime border with Canada and then an extensive northern land border. There are many, many initiatives, some we have talked about today, and in other meetings for port security, the Container Security Initiative, for which we have negotiated, the last time I heard, with 17 of the major mega ports, of the 20 in the world that our people be there on the ground when containers are loaded before they come toward our United States ports.

The Customs Trade Partnership Against Terrorism, the Coast Guard's 96-hour notice of arrival, and then new technology that would scan containers, radiation portals being one that I can think of, what is the status of the implementation and the coordination of some of these container and vessel tracking initiatives that are so vital to ports like the one I am very close to in Washington.

Dr. MCQUEARY. And that obviously is a very, very important area that is being worked, as I am sure you know. Currently the Border and Transportation Security organization, the directorate as well as the Coast Guard, have the prime responsibility to deal with the issues that you have just talked about and do have the lead on that. I have to tell you today we have not been engaged in any great detail at all from the Science and Technology Directorate standpoint, simply because that work was ongoing at the time when we actually became into existence. But it is an area that I would expect that we will work very closely from the scientific standpoint to make sure that those organizations do have the latest and best scientific capability to decide what would best work, and, in fact, we would work very—if a new program were starting, we would work very closely with them to help establish what the requirements are and provide scientific guidance.

But this one has been underway for a while. And so we are in the mode of trying to catch up, quite frankly.

Ms. DUNN. Good. It sounds like you have the same challenge that we have with multiple jurisdictions and how we divide down that responsibility. There is certainly no shortage of ideas for technological innovations in the new Department. DHS has been inundated we know with funding requests from private companies that have Homeland Security-related technology. I think those of us who serve in the Congress know, and can imagine the burden you are under, because we are getting calls from people in our districts who have all sorts of ideas, and in fact, in my own district, we have had to develop a way to provide input for those firms so that we can take advantage of these ideas.

The chairman of our committee has talked about a technology fair that would bring together people who might have great ideas from the government sector, but also from the private sector. And I am wondering if you know, given the numbers of requests that we are under, how the Department of Homeland Security will, first of all, give access to small business, the voices of small business people, and then once you have developed a system for listening to their ideas, as I said, that fair might be one way of doing it. How will you prioritize these requests?

Dr. MCQUEARY. Well, certainly we will be looking for things that fit in with the, what the national priorities for Homeland Security would be. And that would be a sort of a guiding principle for us. We are also going to use the technology—TSWG. I have used the abbreviation so long—Technical Support Working Group as being—as helping us to prioritize and make the selections, based upon criteria that we would provide, of those that are most promising, and, in addition to that, we will be using that same group to review some 500 e-mails that we have received into our Homeland Security site. And I would say to you that most of those e-mails have come from what appear to be small businesses.

So there is an intense interest by small business in being able to make a contribution. So we intend to evaluate each and every one of those inputs. And it has been more a matter of getting the necessary people resources to be able to look at the things to provide considered and respectful responses to those people who have input.

Ms. DUNN. So should we tell our constituents to e-mail you with their ideas?

Dr. MCQUEARY. Not me. If you would send it to science.technology@dhs.gov. It will definitely get considered. The other issue is we have a broad agency announcement that just came out last week from the Technical Support Working Group that lists many different areas of technological interest that we have from the Science and Technology Directorate standpoint. And that's another very good place for people to examine to see whether their products and capabilities fit in with what we are saying that we are interested in now.

Ms. DUNN. Good. Well, as long as we have access to those source, phone numbers or e-mail addresses, then I think that would be great and it would give us another avenue for them to feel like they are being heard by the government.

Dr. MCQUEARY. And they need to be heard. I fully agree with you.

Ms. DUNN. They do. And certainly, we are looking on the government side looking for the best answers. Along that line, in my home State of Washington, as in many places around the country, I know that local law enforcement officers are desperately seeking technologies to help them do their job of protecting the Nation from future terrorist attacks. Where do you feel the Department of Homeland Security currently is in the development of a nationwide communications network that would allow local law enforcement officials the ability to coordinate with State and Federal offices?

Dr. MCQUEARY. We have just assumed—we, the Science and Technology Directorate, on behalf of the Department, have just assumed responsibility for a project called SAFECOM. If you happen to be familiar with that, that was a part of the e-government initiative that was underway being imagined by the office—OMB and we have just recently had that assigned to us, I shouldn't say assigned to us. We said that we would be happy to take on the responsibility for managing that and a part of that initiative is to begin to work what should be the system architecture for providing a large-scale communications system within the country, one that can cope with

surges such as we saw on 9/11 and being able to deal with emergency situations that that might represent.

So that we can be in a position to guide people that are buying locally, will have guidance standards to be able to use, so that, as people begin to buy new equipment, we can begin to move towards an interoperable communication system, because there are some 44,000 different locations in the country that have their own separate communication systems. And to suddenly launch upon a path that says we fix that very quickly would be a probably too expensive to even contemplate.

Ms. DUNN. Thank you very much. And thank you, Mr. Chairman.

Mr. THORNBERRY. Thank the gentlelady. And I would just mention that one of my intentions is to try to put together information for all members so that they can direct constituents to the right phone number and e-mail sites and so forth with the ideas that they have, because I think the gentlelady raises a very good point, as Ms. Lofgren did, that we all have a number of constituents and groups and companies that are interested in offering their services.

The Chair recognizes the gentleman from Kentucky, Mr. Lucas.

Mr. LUCAS. Thank you, Mr. Chairman. Doctor. Some of the questions I am going to piggyback on, but we talked about, you know, the country revolves around cell phones, it seems like. And is there any work being done on any kind of an override capacity, where emergency personnel and the local officials could get through with cell phones as opposed to—anything like that at all?

Dr. MCQUEARY. There is a government system that is called Government Electronic—GETS, I have forgotten what the acronym stands for—that that capacity exists now. So it is known how to do such a thing. If there is any specific work going on to make it be readily available to people that are at the local level, I can't answer the question, but I will find out.

Mr. LUCAS. We don't know that it is workable? I mean, it hasn't ever been tried?

Dr. MCQUEARY. I have been led to believe that it has been tried enough to believe that it works.

Mr. LUCAS. OK. I didn't know if something happened next week, if they could put it into effect.

Dr. MCQUEARY. I think it is the number of people that can actually access it is not sufficient if you had a national emergency.

Mr. LUCAS. Along with Ms. Dunn, we have so many people contacting us, vendors with ideas and technology. And you mentioned that they can contact by e-mail, science.technology@DHS.gov. Is there any other communication that they can go through, or any phone number?

Dr. MCQUEARY. Well, we do have a Web site too, that has some information, although that is more informational than anything else. And then the broad agency announcement I touched upon earlier that is being managed for us by the Technical Support Working Group. That would be another path they can use. That is Web-site based. You can enter the whole proposal in at the Web site and track what is being done with it as it is being evaluated and considered, too.

So those would be the two. And here is that Web site. It is www.tswg.gov.

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

Mr. THORNBERRY. Thank the gentleman.

Dr. MCQUEARY. I would give you my own telephone number, but my telephone is ringing off the wall already.

Mr. THORNBERRY. Please don't do that. We need you to do the job.

The Chair would yield to the distinguished chairman of the Science Committee, Mr. Boehlert.

Mr. BOEHLERT. Thank you very much, Mr. Chairman. And welcome, Dr. McQueary. I was sort of surprised to learn you have been on the job a couple of weeks now and you don't have all of the answers to all of the questions. Is that supposed to comfort me?

No, I am just kidding you, obviously. I really appreciate that.

But let me take advantage of this opportunity, putting on another hat that I wear as Science Committee chair. We have some outstanding requests for you, and I just would like to remind you. One we wrote to the President back in January, before you were on the horizon, about the impact of the transfer of life science programs to DHS, and posed several questions. Then we have provided that letter to your people. And we would like to get some answers to those questions to see how you intend to proceed. That is one.

Number two, a passion of mine: Cargo Mate. We are still awaiting some sort of additional contact on that, because Mr. Chairman and members of the committee, this is a way to track cargo in ports, and you can pinpoint where it is at any given time, which is I think a very valuable resource in providing port protection.

So I would remind you of those two. If you can get back in a timely manner.

Mr. BOEHLERT. Now, let me ask specifically. You have testified before and said a number of times that your job is going to be one of management and that you are going to tap the scientific and engineering expertise that exists in our universities and in the private sector and other government agencies to do the critical homeland defense research and development, such as work on cybersecurity.

How do you go about using these groups? Do you have specific ideas?

Dr. MCQUEARY. Well, specifically, we will be issuing a number of contracts for work. We will be issuing RFPs, we will issue broad agency announcements for people to respond to.

Mr. BOEHLERT. Do you have a feeling for a timetable yet?

Dr. MCQUEARY. Well, we have the one BAA out right now. The money for fiscal year 2003 is largely committed at this point. There is very little opportunity for anyone to bid on new programs other than through the BAA that we have. Certainly there is going to be a very large opportunity, if our budget is approved as presented for fiscal year 2004, in which we have $803 million proposed at this time to—

Mr. BOEHLERT. Do you have any idea how much, like on a percentage basis, a guesstimate—I wouldn't expect a precise figure—on how much of your external funds will go to activities research, activities at universities and the university community?

Dr. MCQUEARY. Well, in the very beginning it is my considered professional judgment that we need to be focusing our energies on things where we can bring answers to bear quickly. That is not to say that we should neglect the longer-term research issues, because there are some areas that do need that.

But in terms of economic balance, I would expect that most of our energies are going to be on things that can be accomplished quickly, and then we can evolve into what I will call a more steady-state operation in which we have a balance between ongoing activities as well as those looking to the future.

But right now, we have a number of things that I am confident we can do, based upon the limited amount of exposure I have had to what is going on in America, that we can bring to bear some real answers quickly.

Mr. BOEHLERT. I would agree with that analysis on priorities, the short term immediately.

Do you envision providing any funds to other agencies like NSF or NIST or NIH, or do you think they have sufficient resources to do what they need to do?

Dr. MCQUEARY. I believe that—and I could be convinced otherwise—but I believe those organizations have sufficient funds in their areas. We do have agreements as to how we would work with them in most if not all cases.

Mr. BOEHLERT. I am comforted by the fact that you do have a good working relationship with these other agencies. I assume you are strengthening that as each passing day goes by.

Dr. MCQUEARY. Absolutely.

Mr. BOEHLERT. I think we do expect miracles from you guys. You have got a very demanding job in a very difficult time period with some real challenges on the horizon, and we expect instant results. Just go forward, knowing that you have a lot of support from Capitol Hill, from people who appreciate people like you with outstanding records of service and bringing a lot to the table as you have come to take on this most challenging and demanding position.

Let me ask you one other thing. Talking about communications systems and "interoperability" is the big deal. That is the big word. Talk a little bit about that, will you? We know, for example, in 9/11 with the Twin Towers down, it was a hell of a difficult problem that we were not able to overcome in having interoperable communications systems, so that one can talk to the other and get the message through.

Dr. MCQUEARY. Well, the fundamental problem as I understand it there—and I was not close to it, so I don't want to go very far and prove that I don't know what I am talking about—but when you design a communications system, you have to design what kind of peak load capacity you expect that system is going to have to accommodate. And, in general, you make accommodations for that. When I worked for AT&T, Mother's Day used to be the most active calling day of the year for communications. So we always had to make sure that you could get through rather quickly if you are trying to call your mother.

I doubt that anyone would have conceived of trying to design a wireless communications system for New York that could have ac-

commodated what had to have transpired when that awful tragedy occurred. And so I think the answer for such a system would be one that was touched upon earlier: Is there some kind of priority so that those who really do need to get through to make calls can indeed make them? I do believe that there are ways of accomplishing that.

Mr. BOEHLERT. Thank you very much. Mr. Chairman, thank you for the time.

Just let me pass with one observation. Those of us who have come to know Dr. McQueary know that he is a good guy with outstanding credentials, and he brings something very important to public service. But how refreshing it is to have a witness of your distinction who on occasion will say, "Gee, I don't have the answer to that one, I am trying to figure it out myself." We are all trying to figure out a lot of things.

Mr. THORNBERRY. The Chair appreciates the chairman's comments. It is reassuring to me, too.

The Chair recognize the gentleman from Florida, Mr. Meek.

Mr. MEEK. Thank you very much, Mr. Chairman. Thank you for being here today, Mr. Secretary.

I had a question along the lines of communications. We can talk about cyberspace and get even into a bigger conversation as it relates to servicing your customers. I was reading over your opening statements, and I am sorry that I missed it. I am on the Armed Services Committee and the bill is on the floor now.

The folks back in Florida where I am from, one of the biggest concerns they have, outside of many others, is the issue of communications. And we know now, many of us in this committee room, we have Blackberrys and cell phones and whatever, even is touching their Palm these days. But the average American, they just have simply the home phone. And if something was to happen, especially when first responders are trying to respond to a scene or contain a bad situation, if it is in a downtown area, big or small town, many of the people will not know of what is going on and what they should do at that particular time.

Does the Department have the technology to notify individuals—let's say, for instance, USA America City, medium-sized city, has a downtown area; if we were to have a terrorist attack at a building, you wanted to keep everyone in the building or out of the building, how would the Department contact those individuals or how would—do we have functions locally?

Dr. MCQUEARY. That activity would be managed by FEMA. And I have to tell you that I don't know the details of all of their communications capability right now. But certainly what you are describing is something that, if we have not adequately addressed, it does need to be addressed.

I have seen, in fact, proposals that have come in during this time of people sending in to our e-mail address that I alluded to earlier, in which people believe that they have possible solutions for that. We have not had a chance to evaluate those to determine whether they have efficacy or not.

Mr. MEEK. That is a very serious issue because, being a past first responder myself, I know that in the early stages of any incident

it is important, need it be trauma care or need it be direction to the general public.

One of the things that I think is important, and myself and other members on the Homeland Security Committee, we are going to draw up a bill tomorrow. But you may already have this authorization—I don't know—to be able to allow the Department, on the discretion of the Secretary, to contract with a telecommunications company to be able to call people or call an office building when you need to be able to share pertinent information with them, need it be in a city, in a block grid, need it be across America so that people will know. I have heard all kind of different ways that we can do this, through weather radios and, I mean, you name it. I am pretty sure that you have a bunch of ideas either stuck in your e-mail or on your desk right now, waiting for folks to review.

But, I think it is important that we get to that as soon as possible. Do you have that ability now to do that? I know some cities have moved forward saying, go on to our Web site, we will e-mail you or Blackberry you if there is an emergency in our county or what have you. But the average American doesn't have that technology. And how would they be notified?

I mean, if something was to happen now, of course, our Blackberrys will go off. But we have no way of knowing unless someone tells us.

Dr. MCQUEARY. Well, certainly many Americans only have a phone and/or television, or some may not have either one. So it depends on the range of how you contemplate notification, and if one goal is to the full extent you must be able to notify every person independently whether they have a communication device or not, that probably becomes a very challenging, if not unworkable, kind of system to deal with.

Mr. MEEK. That capability is available. Over 86 percent of Americans do have at least one hard line in their home or work where they can be contacted. And I think communications is key, especially some of the exercises the Department has done recently.

That kind of bioterrorism, what have you, is important. I am not saying that you are saying—that you are not saying that it is—but communications. And so while you all are looking at research and development, maybe talk with some of the people in one of the industries. I know you mentioned your background there in the telecom industry.

Those that I have been in contact with said that at the drop of a hat—and people can be contacted, need it be a public line or a private line that is in their home, probably go as far as a cell phone if that could happen.

I think communications is key in this new era that we are moving into. We can talk about being on line or having the technology, or investing 100 or $300 in some sort of hand-carried computer. But Mr. and Mrs. Smith, they are waiting on the phone to ring. If the phone doesn't ring—forget about them being at home, I am talking about if they are at work, they can be there—on 9/11, you read some of the stories; it took people a long time for a lot of folks before they knew what was going on.

So communications is important. I just want you to be able to service your customers well. So I want you to take that as an idea.

Hopefully you all can be in support of the legislation when it comes out.

Thank you, Mr. Chairman.

Mr. THORNBERRY. The Chair thanks the gentleman. And one of the things that we may consider in this subcommittee is some sort of a briefing for members on this first responder communication issue, because obviously there is a lot of interest. We have heard everything from dedicated spectrum to priority calling, to a whole variety of technologies.

At least for my purposes, I need someone to kind of give me the range of options and help put this whole thing in context. We heard a lot about this when Secretary Ridge testified in front of the whole committee yesterday. And I don't know exactly who the best folks are, but I think that would be a helpful thing for me to understand, the range of the technologies. We may pursue that.

The Chair recognizes the gentleman from Michigan, Mr. Camp.

Mr. CAMP. Thank you, Mr. Chairman. Thank you, Doctor. As chairman of the Border and Infrastructure Subcommittee, it is clear that we don't have enough people or facilities to really make the kinds of security arrangements that we need to make, and technology is going to be a critical part of that.

And I wonder, to what extent you have begun working with Customs and Border Patrol and Immigration—as you know, those systems don't talk to one another, the computer systems—and to what extent, now that Immigration is really in two separate agencies, to what extent you have begun trying to get the agencies to be able to communicate together. And if it hasn't begun, do you have any sort of time line in terms of when you are going to begin to start doing that?

Dr. MCQUEARY. Well, the key thing that we have done to date is that we are the lead systems engineer role in science and technology, for the U.S. VISIT system. So we are very closely partnered with the Border and Transportation Security Directorate. And that touches, I believe, upon most of the elements that you talked about. That is the most significant thing that we have going on at this point. We have begun some investigations looking at unmanned aerial vehicles, too, as having possible application there.

But in working the issue of trying to foster further communications among those agents, I, quite frankly—I would suggest that Secretary Hutchinson probably has that high on his own list to make that happen. I would be more than happy to assist him in any way, but I wouldn't be presumptuous enough to try to go and take on that role unless he called upon me to do so.

Mr. CAMP. We hope to be hearing from him pretty soon as well. I know you touched on the university-based centers that are mentioned in the Homeland Security Act. And I just wonder, did you answer how many centers you expect to establish?

Dr. MCQUEARY. We have not determined at this point. In fact, I don't think it will be as many as ten; it will be more than one. But we have not reached any kind of a firm conclusion. We have begun looking at what the criteria need to be and also, as I mentioned earlier, working with National Science Foundation, American Association of Universities, and American Association for the

Advancement of Science to help us sift through recommendations as which universities would be the logically ones.

And by the way, it doesn't necessarily have to be just a university. I can envision where more than one university might get together to have a partnership of two or three or more, that would be stronger than just any one, and have that designated as a Center of Excellence. So we are not pinned down to the idea of a university Center of Excellence only.

Mr. CAMP. Thank you. I want to add my voice to the chorus you have heard about the inquiries we are getting from companies, individuals, who really have ideas to improve our security. And I appreciate knowing about the Web sites.

But can you tell me a little bit more about what happens once an individual or a small business might sign up on one on of these Web sites, the process from there on? Are they contacted and things of that nature?

Dr. MCQUEARY. 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 were doing. So we gave out the e-mail address in an interview that I had with a newspaper a couple of months ago, maybe 3 months ago at this point.

And after that was done, we just were flooded with inputs through this, because lots of people read this particular newspaper. And what we do with those, I actually read every one of them myself. And when I say I read them, those that are many pages long, I only read the executive summary to get a sense of what is there.

Some of them are so intriguing that I will immediately send them to one of my associates and say, Please take a look at this, because it looks like something we can use.

Others will simply say—I had one that said, Please tell me what you are interested in and we will let you know whether we have anything. It didn't take too long to deal with that particular one.

And then I had one from a high school student that I responded to him myself, because I thought if a high school student would write to me that he deserved to have an answer from me.

Mr. CAMP. So are you expecting, then, a sort of formal review procedure that—with a certification attached to it?

Dr. MCQUEARY. We will use the Technical Support Working Group as the formal review and certification, and listen to their recommendations as to what we should pursue and fund as a result of that review.

Mr. CAMP. All right. Thank you. Thank you very much. I appreciated your testimony. And thank you, Mr. Chairman.

Mr. THORNBERRY. The Chair appreciates the gentleman. The subcommittee is very pleased to have the Ranking Member of the full committee, the gentleman from Texas, Mr. Turner. The Chair would yield to him for any questions he may have.

Mr. TURNER. Thank you, Mr. Chairman. Thank you, Dr. McQueary for being with us today. I am sure it has been a whirlwind to have taken over this responsibility just a few weeks ago.

I notice that you have about 50 people on board, and I assume that will grow. I don't know if it can grow in the current budget or whether it will take the next budget cycle for that to happen.

Dr. MCQUEARY. We have approval for 79 FTEs in our current fiscal year 2003 budget. We expect to take that to 180, assuming our 2004 budget is approved as presented.

Mr. TURNER. I know Ms. Christensen asked a question about Project Bioshield. And I gather you haven't had a chance to take a look at the legislation that was before our committee recently on that subject, and I don't know if there is somebody within your operation that has. There are some issues there that our committee needs your help on because the bill was referred to us because of the role that the Department of Homeland Security has in trying to develop biodefenses.

It seems to me that we are in the state now where we need to be sure that as we carry out our role with respect to the Bioshield legislation. I believe we have crafted that legislation in a way that is consistent with the objectives and the statutory directives of your Department has, including in the Information Analysis Directorate where they gather intelligence about the biothreats.

In your statement that you have given the committee today, you have set out two specific roles that you will have. One is the deployment of the biological warning and incident characterization system, which I gather is an effort to try to detect the presence of biological agents.

Dr. MCQUEARY. That is correct.

Mr. TURNER. Then you also mention the National Biodefense Analysis and Countermeasures Center.

Dr. MCQUEARY. Yes.

Mr. TURNER. You state in your opening statement that that Center will leverage the expertise of America's cutting medical and biotechnical infrastructure to focus on the biological agent threat, including performing risk assessments. You say it is an essential new approach to integrating national resources for homeland security supporting public health and law enforcement. You go on to say that the analytical capabilities will be functional in 2004 and coordinated with the National Institutes of Health and the Food and Drug Administration. Is that correct?

Dr. MCQUEARY. That is correct.

Mr. TURNER. That section, that biological warning system and the National Biodefense Analysis Countermeasures Center, represents, really, the largest section of your 2004 budget request, $265 million.

Dr. MCQUEARY. 365.

Mr. TURNER. Excuse me, 365. Now, what I think we are struggling with on this committee is trying to be sure that we understand the role of this Center, the Biodefense Analysis and Countermeasures Center, and how this fits in with the other agencies that are already in existence, like the Centers for Disease Control, National Institutes of Health, and try to make some logical assessment of whether we have divided up this responsibility properly and what it is that we are going to accomplish.

I have several questions that come to my mind. Maybe you can respond to all of them at once. I am trying to figure out, first, what role the Biodefense Analysis Countermeasure Center has with respect to Project Bioshield, which is the legislation before us.

Second, will the Center, be responsible for developing vaccines or other medical countermeasures to biological threats? That is, will your Center be in charge of assessing likely biological threats, or is that role carried out by the Information Analysis Directorate?

Third, once the threats have been assessed and determined, will it be the Department of Homeland Security's role to trigger the procurement of the vaccines we hope to develop through Project Bioshield?

Last does the work of the Center duplicate or compliment the work that is being done at other centers, like NIH, Centers for Disease Control, and the Army's Medical Research Institute for Infectious Diseases?

I know that I have given you a lot of questions, but we need to explore these issues in depth so that when we pass that legislation out of this committee, we have taken care of the homeland security piece of Project Bioshield.

Dr. MCQUEARY. Let me give you a partial answer, and then suggest perhaps that some of my staff can get together with yours to understand in detail the issues that you have so that we can provide a reasoned and thoughtful response to that.

But first of all, my intent, to the maximum extent that we can, is to make sure that we do not have duplicative efforts elsewhere. My intent is to try to be sure that we take advantage of what the government has paid for, what industry has already done, and not engage in duplicative work, because of the point that was made earlier that is wasteful of resources, and we never have enough resources to do all of the things that we want to do. That is point number one.

The role that we expect to play in each of these areas that engage—whether it is NIH or any part of HHS or USDA, our role is to—the things that we would be funding is what I will call to fill gaps that are not currently being investigated in other areas. So part of our responsibility is to make sure that we have a close enough relationship to the work that is going on relative to homeland security in these agencies so that we can determine where we might make contributions.

And, specifically, and the things that you are talking about, is the areas that we would expect to be fully engaged in: the threat analysis in concert with the IAIP, as you correctly observed. We would expect to be engaged in establishing what the prioritization of threats would be from the scientific standpoint. And we would certainly be involved in the details of acquisition strategy and setting the requirements for whatever it would be that we would ultimately buy to assist homeland security.

So I think if you think of those three things, it is not really something that NIH or other parts of HHS or USDA would normally be doing as they support homeland security.

Mr. TURNER. Well, I think if that is your intent, I think we probably need to be sure that is included in the Project Bioshield legislation, because I think there is competition for those roles.

I respect very much what you said and we certainly don't want to duplicate activities within the government. But I am not sure that it is clear what role the Department will play. But I approve of what you said and I agree that it is your responsibility to assess

the biological threat. I think it is your responsibility to set the priorities of which threats we should deal with first, and in what order. And I think the issue of decisionmaking about procurement may very well be your responsibility as well. I wish you would work with us on this, because we are on a tight time frame.

And you know, I even think it would be appropriate for the Department to take an even stronger role, and I suggested this in the hearing, because Project Bioshield, as currently drafted, envisions that we will find a private sector answer to developing vaccines in every instance.

And we have had some people share with this committee their views that we need to find such an answer as a first step, but we also need to be willing to have some entity within the Federal Government, not necessarily within the Department of Homeland Security—but it could be—where the research is taking place to try to find and discover the vaccines that we need to deal with these dangerous biological agents.

And if that is a view that you share, we need to hear that: Otherwise, we have placed all of our eggs in the basket of counting on the private sector and the drug companies to step forward to solve these problems for us. There are some people who have suggested that such an approach may not work. If it doesn't work, we have lost valuable time in addressing these threats.

Dr. MCQUEARY. Sure.

Mr. TURNER. And any ideas you have on that, I certainly want us to have the benefit of them as we try to move forward on this bill.

Dr. MCQUEARY. I will be happy to engage in a discussion with our folks about that and get to you in short order, because it is an important question.

Mr. TURNER. Thank you, Doctor.

Mr. THORNBERRY. Thank the gentleman. The subcommittee is very pleased to have the Chairman of the full committee, the gentleman from California. He is recognized.

Mr. COX. Thank you, Mr. Chairman. Welcome, Dr. McQueary.

This is, of course, the Subcommittee on Cybersecurity, as well as Science, Research and Development. And we have structured the subcommittee in this fashion because it seemed so clear that there has to be a relationship between ongoing R&D and the deployment of cybersecurity countermeasures in real-time if we are going to succeed in that area of our mission.

Unlike almost all other aspects of national security, cyber doesn't sit still, particularly as compared to the old paradigm of guns, guards, and so on. We have to commit ourselves to making a constant investment in cyber almost every day you wonder if the measures that you had in place yesterday are going to be good today. The speed of change and the number of participants in making that change happen really has no analog or precedent in the history of warfare.

As a result, I am very interested in what Secretary Ridge told us yesterday; specifically, that he is going to create inside the Information Analysis and Infrastructure Protection Directorate, a division for cybersecurity. And I am particularly interested in asking

you, since you are here today, how you are going to interact with that division.

Dr. MCQUEARY. Our responsibility will be to support them with the very best science and technology that they need in order to accomplish that. And we do have people that are experienced in cybersecurity on my staff. We have one person at least that is detailed to us from the IAIP organization, and so we will be closely coupled with the IAIP group; but they will have the lead, and we will support them in any way that we can based upon the scientific capability that we have.

Mr. COX. Do you have cyber priority within your ambit?

Dr. MCQUEARY. We have, within our budget this year and proposed budget for next year, moneys that were intended to be in a support role. I would hasten to say that our budget was put together when the Critical Infrastructure Board existed, and therefore we may end up having to relook at that, whether we do have enough allocated. But we would certainly come back to you before doing anything, obviously.

Mr. COX. The reason I ask that question is that in your written testimony there isn't any mention of it. In the budget allocations that you have laid out to us, which you submitted to us in writing, we have the largest amount for bio. And then we have amounts for chem, high explosives, radiological, nuclear. And the smallest amount, only $5 million is for IT. I take it that must be the vessel in which you are thinking of cyber, the subset of the smallest amount that has been requested. It seems essentially trivial. And that may be appropriate, because it may be that is someone else's business and not yours.

Dr. MCQUEARY. Well, we will provide the support that is needed for IAIP. Keep in mind the 2003 budget was put together last year before the Department ever existed, and essentially the same thing—well, the same thing with the 2004 budget, too. And at the time when the 2004 budget was created, the President's Center for Infrastructure Protection existed at that time, and it was believed, we believed, our people putting together the budget believed, that the major leadership role was going to be there. And so quite frankly we didn't know in detail what the responsibility was going to be for science and technology other than there was a view that we would probably be called upon for some scientific support.

With that responsibility now focused in the IAIP Directorate, we will provide whatever support is needed in that very important area. Because if we need to revisit the budget in order to accomplish that, that is what we will do.

Mr. COX. When we wrote the Homeland Security Act legislation, as it was moving through Congress one of the things that was in flux was the name of the IAIP Directorate, and in fact for a time the first word in that directorate was cybersecurity. That was true on the House floor, in fact.

We always intended, in any case, that that be a huge piece of that directorate. And so I am not disturbed that that is where it is going on at all. That is where Congress intended it to go on. But what I want to be sure of is that to the extent that developmental R&D investment, ongoing imagining about what comes next as a part of that mission, that if you are not doing it, they are equipped

to do essentially what you are doing in these other areas such as bio, chem, radiological and so on.

When it comes to cyber, are they going to be able to do essentially your mission inside their directorate when it comes to cyber?

Dr. MCQUEARY. We are obviously two separate directorates and will supply the number of people needed in order to support the mission they have for cybersecurity.

Mr. COX. Except that you have to make decisions. You are planning. You are asking Congress for money, presumably you are going to get it. When that happens, you are going to get the biggest slug of money for bio. With my limited imagination, I can't see how a whole lot of that is going to be useful for cybersecurity, although everything is ultimately connected.

And the same with chemical and the same with high explosives and so on. Those are different silos. And by the time we get down to IP, you are asking for $5 million, and that includes infrastructure protection per se, not just the subset that is IP via IT attacks. And so there really isn't going to be much in the way of significant resources within your area for this because we haven't asked for it.

Dr. MCQUEARY. And I will say once more, if we find collectively—and I include the Congress in that evaluation—that the amount that we have in there is inadequate, then we will find a way to recommend that we reprogram the budget in order the put more money into that area. But right now the largest—

Mr. COX. That wouldn't be necessary, Dr. McQueary, if it were adequately provided for in IAIP. And so it may be that it is not fair to ask you about what is going on there. But I need to know from somebody at some point whether or not that is being provided for within that directorate.

Dr. MCQUEARY. Right. And I think we owe you that answer. And I can't answer for them, because I don't know what the budget number is for them.

Mr. COX. All right.

The second, and I think in the interests of time, Mr. Chairman, the last area that I will open up is the question of how you are prioritizing threat analysis within S&T, because, of course, that is one of the responsibilities that you have undertaken.

Particularly, you have that interest with bio. I think Mr. Turner touched on that a little bit. How are you getting threat analysis to be prioritized within your area?

Dr. MCQUEARY. Well, first of all, we have—what we have taken is the—what are called the threats that can obviously do the greatest damage to the country as being very high on our prioritization. And the biological threat as well as the nuclear threat are the two that can do the most damage with a single incident, and, therefore, that is why those have such high priority in terms of the proposed investment strategy. That is not to say that the other areas in chemical and radiological as well as high explosives should be ignored, because they should not be, because, quite frankly, the most likely thing that we may be faced with is someone deciding that they are going to set off one of those three kinds of devices.

But in terms of damage that one can do to the country, setting off a large—a nuclear weapon of almost any size in a largely popu-

lated area would do more enormous damage than any one of the other three, if you had them, all three, coming at the same time.

Mr. COX. What is the source for that threat analysis?

Dr. MCQUEARY. Just simply looking at—if you had— Sandia and Lawrence Livermore have both done analysis that would support the idea that if you set off a multikiloton nuclear weapon in New York City, it doesn't take much imagination to know what kind of kill radius one would have and how many people can be damaged in that area.

Mr. COX. Maybe you mean it exactly that way, the answer you just gave, but I am not sure. What I mean is, are we relying on Sandia for the threat analysis, or where is the threat analysis coming from?

Dr. MCQUEARY. Well, the detailed nuclear effects work would certainly come—I would call it DOE, because that is traditionally where that analysis has been done. And the country relies upon the expertise that is in those areas to provide that.

Mr. COX. I ask this question because the statute requires analytical capability within—inside the Department, and it is not there yet. It is a work in progress. We have other sources of information for the threat analysis. And then, second, you are responsible, according to the law and your testimony here, for prioritizing the R&D work on countermeasures. And so you have got to do a second level of prioritization, once we go through the threat analysis. If this is the chemical threat, then these countermeasures are more worth pursuing than the next level, the next level and so on. I am reasonably confident that you can do the latter, and that you are doing the latter, although I would be interested in hearing an explanation of how, and I am not at all sure about the former. And I suspect we must be getting it over the transom in the short run, because we can't do it in-house.

Dr. MCQUEARY. Well, I think I answered a question that you did not ask. I apologize for that.

Mr. COX. I apologize for not asking the question clearly enough.

Dr. MCQUEARY. We do participate in prioritizing what the threat would be. And looking at—we view the nuclear weapon incident as low priority, but the—as low likelihood of happening, but the potential damage is enormous.

Similarly, maybe higher likelihood of incidence, but with biologics enormous damage could be done to the country through that, and, therefore, you take the combination of likelihood of happening and weigh that with the damage that can be done, and the combination of those two things assist us in deciding where the priority should be and what the expenditures should be accordingly.

Mr. COX. There may be less difficulty in imagining the ultimately devastating effects of a nuclear detonation. But with respect to the likelihood, which is a question of, among other things, capabilities of various people, groups, individuals, where are we getting that information in the short run right now?

Dr. MCQUEARY. Well, in the short term, that is really a discussion that probably should be handled in a classified setting.

Mr. COX. I don't mean that. I mean, which part of the government?

Dr. MCQUEARY. Well, directly, the experts in this are at Sandia and Lawrence Livermore. I mean, the experts in knowing what the consequential damage would be for a nuclear weapon detonation would come from those organizations.

Mr. COX. With respect to the likelihood question, the rest of the analysis, the likelihood of that as opposed to another kind of attack and the capabilities of real enemies as opposed to what just in theory might happen, does that also come from Sandia?

Dr. MCQUEARY. No. The likelihood has to come out and will come out of the IAIP, the Information Analysis and Infrastructure Protection Directorate.

Mr. COX. Is that happening right now? Are you getting that kind of information from IAIP?

Dr. MCQUEARY. Just a moment.

Okay. The—the answer is we—I participate weekly, twice a week, in threat analysis briefings, and we have people in our organization, as I mentioned earlier, that came out of the infrastructure analysis and protection group. That group worked very, very closely in the formation of—when the homeland security organization was being put together, the IAIP and the science and technology groups were co-located in the same location. In fact, you have a gentleman behind you there that was an integral part of helping work the IAIP piece of this. So there has been, and continues to be, a very close collaboration between the two organizations.

I have not personally sat down and reviewed detailed material that has been presented, and so I am not knowledgeable enough to be able to speak to that.

Mr. COX. Are you getting information out of T–TIC?

Dr. MCQUEARY. T–TIC is a very important part of what the threat would be, yes.

Mr. COX. All right. I thank you, Mr. Chairman. And I particularly appreciate your willingness to keep considering the cyber question. Possibly we can follow up in writing or over the telephone even just to learn how the R&D piece of this is getting handled when it comes to cyber, because I can see from your presentation that it is not a big money piece of your operation. But your willingness to do it, if Congress wants to push it that way, is much appreciated.

Thank you, Mr. Chairman.

Mr. THORNBERRY. Appreciate the chairman's comments.

Dr. McQueary, I wanted to follow up with a number of topics that have been raised today, if you don't mind. One of them is that yesterday in his testimony before the full committee, Secretary Ridge said that one of the first priorities of your directorate is radiological detection. And in your comments with the chairman, you alluded to part of the reason that is true: the tremendous devastation that can come.

But as I looked through your outline of how much money is going into each of the seven areas, it doesn't look like it is as high as the Secretary seemed to indicate that it was yesterday. Now, is that—am I right about that? Is it because you have only a limited number of places to put money at this stage? Or how is that—where—how is that prioritization working, particularly on radiological detection?

Dr. MCQUEARY. Well, to answer the question, if I may, in a general sense, the—when you look at what kind of budget you need to attack one of these things, one of the key issues is how complex is the problem that needs to be examined, and that weighs into the challenges, too. And certainly the work that we need to do in the biological area is one of the more complex, because of the short time scale that one has there. So that weighs into helping us determine what the distribution of funding can be.

We had what we call portfolio managers responsible for each one of these areas. We asked them to put together detailed plans as to what they believed the investment program should be. That was reviewed by the program plans and budgeting organizations within Science and Technology, and then ultimately I have the responsibility for what was submitted to that.

But I am comfortable, as we speak today, with where—what the priorities are as laid out. But since this is a very complex, fast-moving kind of threats that we are dealing with, I think it is very important that we recognize that should we conclude that the distribution of funding is inappropriate, than we have a responsibility to come back to you and others to recommend that we make a change in that, because I am not so wedded to any budget that I believe this is the only one that is there. I think it has to be continually evaluated. But we do believe that is the right one, given the circumstances of where we are today.

Mr. THORNBERRY. I appreciate that. As you know, among others on the full committee, the chairman of the Homeland Security Appropriations Subcommittee is a member, and I think all members of this committee and his committee are willing to—are interested in changes that you may want to make, or different prioritizations, different opportunities, because it has been difficult to try to get this up and running and make your allocations. And you haven't been there long. All of those factors we understand. I just think it is important that you feel free to come to the appropriate folks and let us know.

Let me ask you about another one that the Secretary talked about yesterday. He received a lot of questions about the technology to screen cargo in airplanes and whether that existing technology existed, whether further research and development needed to be done. He also talked about that being a high priority of your directorate. What is happening generally in that area?

Dr. MCQUEARY. From what we are doing right now is to understand what capabilities—when I say capability, it may be in the prototype stage—trying to understand what kinds of things already exist and what kinds of things are being contemplated.

Primarily, at least what I have seen so far, is that work is being done in the national labs, and I have seen some very—within the last 2 weeks, I have seen some very interesting technologies that suggest to me that we can make some strides forward in that area. But I am not here today to say that we should launch a program to do one of these things, but I have seen some things that do clearly warrant quick and early examination and determination as to what direction we should go with them.

Mr. THORNBERRY. It occurs to me that in this area, as in the first responder communication area, you have got a lot of folks in the

country that are very anxious to get something done. Your challenge is how patient you are to get it better versus getting something out there. You have had an exchange earlier with somebody about it. That is a difficult balance to get. I don't envy your job at all.

Let me ask, going back to where Ms. Lofgren began the questioning, about how you look at various ideas and products and services that people have. And you have given us some information that we will certainly get around to our colleagues throughout the House. But you clearly have a very important role for the Technical Support Working Group.

There are those that have a little bit of concern about that. Number one, it is under the Department of State, technically, to oversee it. second, you have got folks from a variety of agencies that sit on this group, and the fear is that you may be end up with the least common denominator, and you are certainly not going to have anybody willing to stick their neck out on anything that is really innovative. They are going to end up with a more conventional approach to problems, and we are going to not explore, as we should, all of the alternatives, particularly if it comes—you know, if it is something outside of the mainstream from some small company.

Does that worry you at all that this interagency group has such a central role in assessing the ideas that come to you?

Dr. MCQUEARY. Well, you always had to worry whether you have gotten the very best idea that comes forth. But I do believe that with the multilevel of review process that we have—and I have worked on the industrial side of things working with the Technical Support Working Group, and have submitted proposals to them in the past, and had proposals evaluated and reviewed, and I didn't always agree with the results that came out of that.

And there may be some in which we don't agree from a homeland security standpoint either, but that is why they are doing a job in support of us rather than taking over the responsibility for that. So we will—through the HSARPA organization is where we will manage the projects that will be selected by the Technical Support Working Group.

So I am satisfied that we have a number of possibilities for review. And my experience would tell me if people, companies, feel that they haven't been fairly treated, they do not generally hesitate to make it known to more senior people in the organizations that they are dealing with on how they feel about that.

It is not a perfect process; it never will be a perfect process. My suspicion will be that we will have far more—in fact, I know this is going to happen without even seeing the results, but we are going to end up with far more inputs with people that probably have more good ideas than we have money to fund. And so it will be a matter of setting priorities, rather than why don't we fund, you know, 2- or 300, and only spend maybe 10- or 15K with each one, which isn't enough to get a good idea launched.

Mr. THORNBERRY. Well, and I think we appreciate the—this was an existing organization, and you had to get moving quickly. So you want to take advantage of it, and I appreciate that. I just think it is important for both—for all of us to be mindful of the concern

that they are not inclined perhaps to be as innovative as we would like, although I am not sure that that is a fair criticism.

One of the things that you were asked about earlier today, or you discussed, is your priorities overall within your directorate. And you mentioned that in the immediate term your priorities are the applied side. What can we do to find things, get technology out there quickly to make us safer, but understanding that the longer-term sort of research is also important? Have you set goals as a percentage of your budget, for example, on how much is basic research, how much—or whatever categories you want to use, longer-term research versus how much is more immediate and applied?

You know, one of the concerns that I have had over the years in the Department of Defense is that we have not adequately put the longer-term R&D money into the programs, and when that happens, it is impossible to catch up. You can't make that deficiency up in the near term. Obviously you are just getting started. You have got immediate priorities. Whether it is this year or over the next 5 years, do you have goals as a percentage of your research budget that would go for this longer-term, more basic kind of research?

Dr. MCQUEARY. We have not established any specific goals at this point. I think it is a little premature to have put out numbers that we would have confidence in at this stage. But I certainly have no difficulty at all that the objective needs to be to have goals in such areas and try to move towards those, because I certainly share your view, that longer-term research is going to be very important to this.

As I think about this system we have to deal with, it is a very complex system, homeland security with all of its inputs and outputs. We have a state, if I may describe it this way, that exists today. As the Science and Technology Directorate, we have to be able to characterize what state we want to move it to; in other words, what its capabilities are going to be. And our huge challenge, in fact the major challenge, that this country has is how do we evolve from where we are today to where we want to be.

To do that we will have to have a combination of evolutionary changes and a combination of revolutionary changes. It would be my judgment that when we get to the final state, which itself will be one that evolves, that we then will move into what will likely be an evolutionary operation.

So we have got to go through evolutionary and revolutionary so we can eventually to get to evolve the system at a rate consistent with whatever the future threats turn out to be.

Mr. THORNBERRY. Well, I guess the challenge is knowing which stage you are in, because each of those stages could last a while.

Let me ask briefly about two other areas. Then I want to yield to my colleagues, because I know that they may have other questions.

Obviously one of the things that is very much in the news today is this incident, single incident, of BSE which was found in Canada.

My understanding is that in June, the Plum Island facility will be transferred to the Department of Homeland Security, and I think that will be in your directorate; is that correct?

Dr. MCQUEARY. That is correct.

Mr. THORNBERRY. Have you looked at all about making sure that the Plum Island facility is able to do whatever needs to be done with livestock diseases that could pose a risk to the health, as well as livestock diseases which could be terrorist-induced and could threaten the country?

Dr. MCQUEARY. I have people that are at Plum Island today, this week. They are reviewing, you know, exactly where we are in preparation for this transition.

We do not have a research program that is identified for Plum Island as of today. And as I am sure you know, our responsibility becomes one of being the landlord in facilities, and USDA will continues it operation as it was planned there, and then we have the option of adding to their programs should we conclude that there are things that need to be done.

At this point we have not developed any programs that we would conclude that we need to conduct there. One thing I will say, though: some newspapers have reported that we were contemplating moving that facility to a biolevel 4. That is simply erroneous information and not based upon any factual reporting or discussion either. It is at biolevel 3; that is where we intend to continue to operate should we do anything.

Mr. THORNBERRY. I am sure that you will do all you can as the landlord to make sure that the other work that they do there continues?

Dr. MCQUEARY. Yes, sir. And the USDA had undertaken a facility study because they have had some problems there. We will continue that to make sure that facility is operated with the integrity that it must be for the important work that it does.

Mr. THORNBERRY. Great. Let me just give you an opportunity to make suggestions to us because, as I mentioned in my opening statement, it was over the course, really, of nearly 2 years that Congress wrote the Homeland Security Act of 2002, and we did not get it perfect. And I wonder if you have specific suggestions off the top of your head today, where maybe some adjustments need to be made in the act, some problems you have already run into. Obviously, an open invitation for you to continue to provide input for us, but is there something that you have run into already that needs some adjustment or tweaking in the law?

Dr. MCQUEARY. There is nothing that I have run into already that I think needs adjusting. In fact, I think I have read the law as you might guess. Knowing I was going to move into this job, I wanted to make sure I had a reasonable understanding of what it was I was getting into, so I have read it several times. I think it is, from a Science and Technology standpoint—I wouldn't comment upon the others because I haven't studied it—I think it is a well-crafted law and that it gives us the flexibility that we need in order to run an effective organization. So I don't view that the way it was put together is an impediment.

The only area that we might come back to you on that I know about today, is this the initiation of the Homeland Security Institute. I think that's a good idea, and I am not sure whether we will want to say that having a sunset clause on that is something that should be done, but I would put that in the category of a minor

item and not a major item. But that is the only thing that has surfaced. And it is too premature today to even say that that should be changed because we are not far enough into it.

Mr. THORNBERRY. When will that get up and running do you think?

Dr. MCQUEARY. We have—for the Homeland Security Institute, we are preparing a request for a proposal right now, and we expect to name an FFRDC, federally Funded Research and Development Center, to have that lead role before the end of this fiscal, or certainly by November.

Mr. THORNBERRY. And the concern has been raised with me to, that if you have a sunset, it may make it hard to recruit top-rate people into that organization. At least a sunset that is three years away. It may be hard to get people to leave their current job and come to the Homeland Security Institute if they know the institute is only going to be around three years or at least has to be renewed, and I do think that that's something that we want to continue to discuss with you.

Dr. MCQUEARY. I think that's an important point, by the way, that you raise. Someone's given you very good advice on that.

Mr. THORNBERRY. I have good people, and I try to listen. The Chair yields to the gentlelady from California.

Ms. LOFGREN. Thank you again.

By the way, I very much agree with the point you just made on the sunset. I think that we need to examine that. I just have a couple of final questions.

Section 302 of the Act really puts you in charge of doing R&D and evaluation and the like, and I assume that your Priority Number 4 on Page 3 really is the implementation of that. And as I have listened—and I think this has been a very helpful hearing. I have been thinking about, how do you separate out the things that we—are obvious from—and harmful, like an atomic bomb, a chemical attack, a biological attack, from what's sort of in the background but if unattended, can cause very serious problems as well.

And that gets me to the question I was about to ask, and now, I will ask it a little bit broader. When the initial set of questions started, and that has to do with biometrics and how—who is going to do the analysis of—what is the best biometric? And I assume that the standards would be reliability, ease of deployment, cost, scalability and probably some other things I haven't thought of, so that we can deploy that in a way that makes sense. And the reason why I am mentioning it is it is similar to the interoperability issue for local law enforcement. People are making decisions right now without good scientific data. And by the time we get around to having you—I realize you have got a million things to do all at once, but by the time we get to this, we may have a bigger problem because decisions have been made.

For example, and I am not saying it is the wrong decision because I don't know, the use of fingerprints in the FBI heavily influences the use of fingerprints as a biometric potentially for the Immigration Service. Except 10 percent of the population can't get their fingerprints taken on the machines, and there is a reliability issue. Is there, you know, something that's quicker, that's cheaper, that's more reliable? I don't know. I mean, various people give me

information about that, but in the area of immigration, right now we have nothing. You know, the State Department just announced that they are going to ask for face-to-face interviews with pictures. I guess that's kind of a biometric. But, you know, if we are worried about attacks, we also need to worry about who is going to be implementing those attacks, and we are mindful that the 19 hijackers did come into the United States to do that damage.

So I am eager for your office to pay attention to the deficits, the technology deficits, in other parts of the Department of Homeland Security, and specifically the area of immigration, and I serve on the Immigration Subcommittee and Judiciary and have for quite some time. And prior to that, I used to teach immigration law and practice immigration law. And it is a mess. It has been a mess for decades. It is still a mess. I worked with the last, you know, confirmed real commissioner, who tried in vain to get a CIO, which he couldn't really get because it is civil service and any—they are nowhere.

And I think if we—one of the unique opportunities you have is to step in and set some standards, do some standard setting. We were told by Secretary Ridge yesterday that there are multiple watch lists that have not been integrated, and if they have not been integrated, they are also not fully shared with those who are making decisions about who should come in and who should not come in.

We know that there are over a 113 different databases in the Immigration Service, and they can't communicate with each other. They are still creating paper files and microfiche. Obviously, you can't do a data search if it is on microfiche. And so, I am hopeful that you will not wait to be asked by diverse elements of the Department, but to take it upon yourself, not to implement because that is not your job, but to provide the standard setting that will allow others to implement in a way that actually works to defend our country, because I think it is very serious that we make the right decisions.

You know, recently, I learned of a situation where we invited Russian scientists to come to the United States to be briefed on how to secure plutonium in Russia, a very important thing for our country. And the scientists were unable to actually come in to get the training that we asked them to take because the visa didn't get processed in time. So, I mean, it is ludicrous, but unfortunately it is routine. So the question is, I mean it is a long and rambling question, but this is a very serious problem. I know that it is not being attended to now. How would you proceed and how could we support you in proceeding to set standards and to assist in the technology deficits of this element of the Department?

Dr. MCQUEARY. Well, first, I believe that the U.S. Visa System will be a—is a very positive step moving in the direction where you are. And I believe Under Secretary Hutchinson—I saw in some recent testimony it said that he believed that a combination of pictures and fingerprints was probably the most likely combination of biometrics to be used. I share that view, considering where we are today. Iris scan is another one that is very important. However, if we look at what we are trying to accomplish, we are trying to determine whether there are people who would do us harm. And we

have a much larger fingerprint database, obviously than we do of iris scans. And so—but that would not say that we should neglect that. I think that we should be constantly looking at other opportunities.

I just read an interesting article yesterday, where DARPA had funded some work on looking at the way people walk as being a possible way of determining who they are. And apparently a college in, I believe it is in Georgia, maybe University of Georgia, had been able to run some tests on a hundred different people—and a hundred is not five billion, but it is a hundred different people in which they were getting about an 80 to 95 percent success rate in being able to identify people.

So I think we have to continually be looking for new ways of improving the quality of determination of who it is that's coming across our border, because we must know the answer to that, and we must know who leaves. That is essential to be done in this Homeland Security protection that we have.

Ms. LOFGREN. If I could follow up. I mean, part of the issue—you're right. We have some data on fingerprints and maybe that's in the end, what we will end up with. But the question we have is not just what we have a record on, because most of the people we have in fingerprints are not looking for visas, they are Americans or they are permanently here, but what is scalable that will connect an individual with an identity, even if it is a false identity, but that will nail that person as a single unit, and we are not doing that today. And the reliability issue, I think is very important. And I would love to see some analysis and I don't have, I mean I have got some guesses, but I don't have a conclusion on what that ought to be, and I would hope that we wouldn't just assume, I mean photographs are easily doctored. And I think that we should look to something that is reliable. And I would look to the scientific community, and you, to try and give us some guidance on that.

And second, and I know we are running out of time, and you have been very indulgent with your time. Is there an opportunity to provide some hardware and software expertise to the immigration function? For example, I just learned, frankly by reading the newspapers, that we are going to try and use the SEVIS system for the new visa program. Well, the SEVIS system is crashing every day already. It doesn't work, and you know, if it did work I would be fine, but it doesn't work. And so I—obviously, we need some additional expertise in this area to be successful. Do you have the capacity to do that?

Dr. MCQUEARY. I don't have the capacity today, but that's not to say that we could not muster the resources, because we are not going to be an organization that has all of its indigenous capacity within our organization. We expect to call upon skilled people in private industry, universities and the like. So we certainly have the capacity to be able to lead such an effort, and, in fact, I mentioned earlier, we have the Systems Engineering Lead working on the US Visa System to help determine what the characteristics of that system should be. So that when the system goes out for a bid, they will be in a stronger position to be able to know what to ask for, and we are participating in that today.

Ms. LOFGREN. Could I ask you, later, to send to the committee kind of where—the steps you have taken so far, on that specific area?

Dr. MCQUEARY. Sure.

Ms. LOFGREN. And then, any additional thoughts you might have that could be done, and how we might be supportive in that area?

Dr. MCQUEARY. Be happy to.

Ms. LOFGREN. I would thank the Chairman for his time, and I don't know if Mr. Turner has additional questions.

Mr. THORNBERRY. I thank the gentlelady. Gentleman from Texas.

Mr. TURNER. Thank you, Mr. Chairman.

Dr. McQueary, I know the hour is getting late here, and I'll try to be brief.

Under Section 861 of the Homeland Security Act, a section called the SAFETY Act, there is a provision that allows contractors with the Department to be granted liability protection so that they will have the incentive to sell certain items to the government which they might not otherwise sell because of the business risk entailed in providing terrorism-related equipment, services, and products. It's the Department's responsibility to implement the regulations to carry that provision out. I have heard from many private contractors, in the defense contracting field that want to do business with the Department, saying that these regulations have not been issued. They are somewhat concerned about that process.

Could you tell me what the status of that undertaking is to get the SAFETY Act regulations issued so that we can know that when we need to procure something it will be available?

Dr. MCQUEARY. I cannot tell you precisely where it is. I can give you a general description, but I can certainly find out in detail and report back to you.

Our intent was to have a private industry have an opportunity to comment upon the regulations to see whether they make sense. Now, the likelihood of getting unanimity of view is not high, but certainly having the input would be very valuable to us. We have internal discussions, in fact, there is—one of our documents that establishes delegation of authority is under review right now, and if it goes through as it has been put together, the authority for deciding who will be given the approval for whatever the act turns out to be, that will likely be assigned to me. And it appears—unless the Secretary decides he wants to do it a different way.

So my input would be, the industry needs to feel free that it should openly provide to us, on what their views are on that. I had someone call me just within the last week on that subject. Turns out it was someone that I knew, wanting to know, saying we are very worried—a major company—we are very worried about this. I said, why don't you send us a letter and tell us what you think about it because we would like to have input? So we don't have—and so that would be beneficial to us.

Mr. TURNER. I might mention to you, as you begin to try to deal with this, that the delegation of whose responsibility this is really hasn't even been made yet. Is it premature to ask who is creating the regulations?

Dr. MCQUEARY. Right.

Mr. TURNER. This was an issue of some controversy when the bill was passed. I will tell you, up front, that I was on the other side of the prevailing side because I advocated a position that the private sector and the defense contractors advocated, which was that the Department should be granted the authority given to the Department of Defense under current law, which allows them to grant indemnity on a negotiated basis, product by product, to the provider. Most of your contractors will tell you that this has worked well in the Department of Defense. But what happened is that point of view that I advocated was defeated when I offered the amendment by one vote on the floor of the House, in favor of the language that is in the bill. You are now required to plow new ground, and to basically certify that a product is safe. Once you have done so, then the provider is home-free with regard to any liability. I thought that was probably an ill-chosen path to try to send the Department down, but if you come to the point where you find that too burdensome, I would urge you to take a look at what the Department of Defense has done for the last 25 years and see if that might not work more smoothly to accomplish this goal. If so, we might find the extra vote we needed on the floor of the House to get it back to the way DOD has handled it.

Dr. MCQUEARY. Yes, sir.

Mr. THORNBERRY. Dr. McQueary, I do appreciate your patience as well. I want to get your impressions in a couple of areas, and then there will be, I am sure, other questions we want to submit in writing.

Obviously, the Homeland Security Department was bringing together 22 different agencies into one entity. My understanding is that there were about 15 different programs that were either created or transferred into your jurisdiction. Generally, how has that management challenge gone during—do you feel? Are we getting them together to work as one unit? It is a very difficult thing, and, obviously, you have had only a limited time to work on it, but what's your general impression about how well that's gone?

Dr. MCQUEARY. My view is, it has been relatively seamless in making the transition. The programs—we are continuing the programs that were being done in DOD. They were good programs, and what we have done is take the programs based upon their character and assign them to our portfolio manager. So we have a lead person reporting into the program plans and budget organization. And that portfolio manager assumed responsibility to continue the work that was going on. And so it seems to have gone quite well from my perspective. In fact, I have had—no difficulties have been brought to my attention about that transition.

Mr. THORNBERRY. Good. One other area. It came up today during a long series of questions from Mr. Weldon.

This concern or interest in being able to transfer technology that may be in the Homeland Security Department, may be in the Department of Defense, may be somewhere else into first responders or somebody else who needs it. Is that something that your directorate will be considering? Identifying technologies that may be somewhere in the government and seeing how and whether it may be appropriate to transfer those to first responders, among others?

Dr. MCQUEARY. Yes, sir. In fact, I have met with Assistant Secretary Paul McHale twice already. He and I have agreed upon a working relationship, from the Department of Defense standpoint, working, having the Homeland Defense Organization. And basically, that organization will be one in which he and I will formally get together on a quarterly basis, and then we will encourage open dialogue between Science and Technology and the Department of Homeland Security and the resources he has in the Department of Defense. So that's a start.

I have also met with Admiral Jay Cohen and the Office of Naval Research to establish, I mean a couple of things. He has provided his people and also been very open about anything they have got that we can bring to bear. And so I put this in the category, when I mentioned earlier, we must understand what's available before we launch into large development programs to do something that could be duplicative. And I think it is fundamental to our responsibility that we do that and do it not only well, but quickly.

Mr. THORNBERRY. Yes. I think that's very encouraging. And then you can, once you have identified if it is appropriate to get it into the hands of firemen or police or whatever, then you are able to do that. So I do think that's encouraging.

I appreciate very much your time today, as well as the efforts that you make. I hope you get a sense that you have a number of members on this subcommittee, but also the full committee who are very hungry to be active partners with you and the Department to help this Department of Homeland Security succeed in making us safer. And we look forward to continuing to work with you toward that goal.

Without objection, the record will remain open for 10 days for additional questions, and we will work with your folks on written responses to those questions.

If there is no further business before the subcommittee, we stand adjourned.

[Whereupon, at 4:22 p.m., the subcommittee was adjourned.]

Materials submitted for the Record

REPONSES TO QUESTIONS FOR THE RECORD FROM UNDER SECRETARY CHARLES E. MCQUEARY FOR THE SUBCOMMITTEE ON CYBERSECURITY, SCIENCE, AND RESEARCH AND DEVELOPMENT FOR A HEARING HELD ON MAY 21, 2003 TITLED "HOMELAND SECURITY SCIENCE AND TECHNOLOGY: PREPARING FOR THE FUTURE"

1. Priority-Setting

a. How were priorities established for each of the seven R&D portfolios described in Department budget documents? What were the major factors that were considered, and how did you arrive at specific funding levels for each portfolio?

Answer S&T 1.a. The priorities within each of the portfolios are the initial responsibility of the portfolio manager, with review and concurrence of those priorities by the Assistant Secretary, Plans, Programs and Budgets, with the ultimate responsibility for these priorities being mine.

Factors that were considered include national assessments of terrorist threats, the national strategy for homeland security, and the state of our ability to detect and deter those threats. Specific funding levels for each portfolio were identified in accordance with our current assessment of the efforts needed to meet our mission and objectives. We will continue to assess both the state of our science and technology and its ability to meet the objectives, and the effort needed to develop and/or demonstrate that technology.

b. Do you anticipate any changes in the near-term in those priorities or in the methods used to set them?

Answer S&T 1.b. We do not anticipate any changes in the near-term for the current priorities of our portfolios nor the methods used to set those priorities. However, we are continuously evaluating the factors used to set our priorities and we will adjust our priorities as necessary to be consistent with those factors.

c. In setting priorities, how does the Directorate use vulnerability, threat, and risk assessments? What methodologies are used in making such assessments and translating them into priorities? What are the potential pitfalls with the approach(es) used and how do you avoid them?

Answer S&T 1.c. We use existing information on threats and vulnerabilities to identify high consequence potential threats. Our work focuses on detecting, deterring, and if necessary, mitigating the impact of a successful attack for these high consequence threats because of the potential they have to cause major loss of life, result in severe economic damage, significantly disrupt our critical infrastructure, or damage national symbols. Our Threat and Vulnerability, Testing and Analysis (TVTA) Portfolio will be the principal provider of these net assessments, working closely with the Department of Homeland Security's (DHS's) Information Analysis and Infrastructure Protection (IAIP) Directorate. These net assessments are then used to help set our priorities. Potential pitfalls to any assessment of threats, vulnerabilities and our current ability to thwart these threats are recognized and include uncertainties in the state of knowledge of the threats and vulnerabilities and a constantly evolving technology base which aids our efforts to counter these threats but may also provide new capabilities to our enemies. Constant and ongoing assessments with independent evaluations offer the best defense against surprise.

d. To develop new countermeasures, the Directorate will need to identify and employ the right mix of activities throughout the R&D pipeline, ranging from long-term, basic research all the way through deployment. For each stage, how will you decide what is the right level of investment in each of these activities, including projects with large potential benefits but high risk of failure?

Answer S&T 1.d. DHS does not break down its Research, Development, Test and Evaluation (RDT&E) efforts into 6.1–6.4 categories like the Department of Defense (DoD). It is safe to say, however, that our initial focus will not be in basic research (6.1), but rather 6.2–6.3 (to use DoD categories). Below is a table that indicates the percentage of fiscal year 2003, fiscal year 2004 and fiscal year 2005 funds that go to basic research, applied research, and development.

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

Fiscal Year	Fiscal Year 2003(actual)	Fiscal Year 2004(estimated)	Fiscal Year 2005(proposed)
Basic	47	117	80
Applied	59	56	229
Developmental	398	608	643
Total	504	781	952
percent basic	9.3 percent	15.0 percent	8.4 percent

Some of the cyber forensics efforts will be basic in nature, as will our efforts in the social sciences (such as behavioral or autonomic indicators of hostile intent, or efforts to develop an understanding of people's reactions to threat warnings.)

In addition, longer-term research efforts are a specific responsibility of the Homeland Security Advanced Research Projects Agency (HSARPA) within the Science and Technology (S&T) Directorate, by their investing in higher risk, higher payoff technology development. Our Emerging Threats Portfolio is designed to foster long-term innovative and creative exploratory RDT&E programs to anticipate and counter new and emerging threats. Both programs will be structured to encourage individuals or teams of researchers to pursue high-risk/high-payoff mission-related projects. In addition, the national laboratories will be expected to leverage and apply the expertise gained from basic science programs supported by the DOE/Office of Science, National Science Foundation, and other government agencies towards the homeland security mission.

To determine the correct mix of basic and applied research, our portfolio managers coordinate with operational end-users and use their expert judgment to define needs and requirements for their research areas.

e. How do you make sure that needed technologies make it all the way through this pipeline—for example, how do you avoid the so-called "death valley" problem, where promising research results are not picked up by industry because of market uncertainties, and at the same time avoid interfering in the marketplace?

Answer S&T 1.e. Capturing the entire range of research and transition activities in one organization helps to ensure the coordination necessary for successful transition to end-users. Constant dialogue with the operational end users, use of proactive solicitation of ideas and products from the private sector through the interagency Technical Support Working Group (TSWG) and Broad Agency Announcements (BAAs) also help us focus our efforts and keep us informed of the current state of technology. The Technology Clearing House will also provide a mechanism for private industry to become aware of available technologies. We will use the Systems Engineering and Development organization within our S&T Directorate to manage this transition process. We also will use independent and objective reviews of our programs to ensure we are meeting the overall mission requirements. Moreover, we have a process through the National Science and Technology Council's Infrastructure Subcommittee to work with the privately owned parts of the critical infrastructure sectors to identify their prioritized requirements. With this process, we are likely to avoid the "death valley" problem as it is industry itself that has identified the need. Through Department of the Treasury lead, the financial sector provided their prioritized R&D agenda in late 2003.

f. Guidelines for merit review of R&D programs—Consistent with the Homeland Security Act's requirement for the Secretary to develop and oversee guidelines for merit review of R&D projects and disseminate research conducted by the Department:

- **Which office within the S&T Directorate is responsible for developing these guidelines?**
- **When will they be completed? If they have been completed, please provide a copy to the Committee.**

Answer S&T 1.f. The development and implementation of guidelines for merit review of research and development (R&D) projects has been assigned to the respective components of the S&T Directorate having responsibility for the selection and execution of our R&D projects. This approach was taken because of the differing nature of the R&D projects; some are more fundamental, some are applied and some are technology development. The Office of Research and Development, HSARPA and the Rapid Prototyping Portfolio are developing and implementing merit review guidelines appropriate to their respective responsibilities.

The Rapid Prototyping Portfolio is using the Technical Support Working Group (TSWG) to help assess the proposals received through that mechanism.

Each of our HSARPA solicitations goes through a rigorous merit review process, using external as well as internal reviewers. HSARPA prefers technical review to peer review. The white papers, proposals and other submissions we ask for require multi-dimensional technology reviews that involve expertise from related fields in science, technology, and engineering. HSARPA Program Managers assemble groups of qualified colleagues to act as reviewers. In the unusual event that they do not have access to a particular expertise, our procedures also allow the engagement of any individual expert from outside the government for this specific purpose. All reviewers are required to sign detailed non-disclosure agreements. In evaluating the proprietary information that private entities entrust to us, we prefer to use the government Program Manager as the lead reviewer on the assembled team, the government Deputy Director as the Source Selection Authority, and the appointed Director exercising total visibility and oversight. HSARPA routinely offers submitters the option of having their proposals reviewed by government-only teams, further ensuring that their valuable proprietary data is not exposed.

The Office of Research and Development (ORD) uses a combination internal-external review process for DOE National Laboratory proposals. Portfolio Managers help to recruit PhD scientists to act as reviewers from both federal agencies and the academic community. These panels conduct a technical review of the proposals. The proposals that are most highly-reviewed are then put through an S&T internal relevance review. Appended to this document (appendix A) are guidelines from ORD on their peer review process.

2. Current Organization of the Directorate

a. For each major organizational unit within the Directorate, please provide its name, the name of the individuals responsible for each unit, and a current telephone number for each such individual.

Answer S&T 2.a. A current organizational chart is appended to this document (Appendix B). The relevant phone numbers are listed in the Office Directory that is contained in Appendix C.

b. Please provide the most current contact information for the S&T Directorate, as well as the appropriate contact information for vendors to use if they wish to bring a product or proposal to the attention of the Department.

Answer S&T 2.b. The most current contact information is contained in Appendix C. We are in the process of creating procedures by which all vendors who wish to bring a product or proposal to the attention of the Department can do so fairly. Currently, HSARPA is evaluating proposals and ideas from vendors who complete the Federal Acquisition Regulations listed at http://www.arnet.gov/far/loadmainre.html, Section 15.605 (Unsolicited Proposals). As our procedures change, we will keep Congress informed.

c. Homeland Security Advanced Research Projects Agency (HSARPA)

- **Has HSARPA been established? If not, when does the Department expect to establish it?**
- **What initial research topics will it focus on?**
- **How will HSARPA be structured and what criteria are you using to determine that?**
- **Please describe the process by which HSARPA establishes research priorities, and the means by which intelligence information is, or will be, communicated to HSARPA to inform its research priorities.**

Answer S&T 2.c. HSARPA was established in March of 2003 when the Department was stood up.

HSARPA's initial research interests will focus on the area of novel and improved chemical and biological sensors. Future solicitations will support research and development in the technical areas of Radiological and Nuclear Countermeasures, Explosives Detection, Critical Infrastructure Protection, Standards, Maritime Surveillance and Security, Borders and Transportation Security, Threat Vulnerability and Threat Assessment, and Emergency Preparedness and Response.

HSARPA is a mission-oriented R&D funding organization within the S&T Directorate. To determine the structure, S&T leadership looked at other government funding organizations, examining their strengths and weaknesses and the similarity or difference in their missions compared to HSARPA. For mission-oriented research, having a technical program manager (PM) empowered to accomplish specific objectives is a key element for success. HSARPA is thus organizing around PMs as the operational level, grouped into technical offices with an experienced senior technical

manager as the Office Director. The Office Directors then report to the HSARPA Director and Deputy Director. In designing its internal processes, HSARPA is focusing on streamlining the paperwork and layers of oversight, while maintaining sufficient management and fiscal control. In start-up mode, program managers have not been grouped into Offices. This is to develop a cross-program and cross-technical area collaborative culture that might be stymied by a rigid office structure in the beginning. Within six months, technical offices will be established.

HSARPA has three missions established in law: to promote revolutionary changes in technologies related to homeland security; to advance development, testing and evaluation and deployment of those technologies; and to accelerate prototyping and development of technologies that redress homeland security vulnerabilities.

To establish research priorities for revolutionary technologies, available technical opportunities are assessed in light of the outcomes that can be expected from the investment dollars available. Priorities are established to achieve the best expected research results from the total research investment.

For the remainder of the HSARPA research program, priorities are established by the Portfolio Managers (located in the Plans, Programs and Budget section of S&T) and followed carefully. Portfolio Managers assess DHS customer needs, use available intelligence reports and products, analyze threats and vulnerabilities, identify potential opportunities, and prioritize their operational needs. HSARPA Program Managers collaborate closely with them to design and to execute programs to satisfy these operational needs.

In establishing HSARPA, serious attention is being paid to hiring and obtaining qualified technical personnel with required security clearances, specification of facilities for proper handling of classified information, and providing electronic links and communications arrangements with intelligence counterparts in other agencies. Being able to handle and secure classified intelligence obtained from those sources is crucial to being able to work at the forefront of technologies related to Homeland Security.

d. Technical Support Working Group (TSWG)

• What is the relationship between the S&T Directorate and the State Department-led TSWG?

• What activities has the TSWG been involved in to date on behalf of the Department?

• You have indicated that the Directorate will develop the technology clearinghouse in collaboration with the TSWG. Please describe how that collaboration will work.

• Which clearinghouse activities will be handled by TSWG and which by the Directorate?

• Does the Department intend to create its own TSWG, or will it continue to have to rely on an entity not formally a part of the Department?

• Some observers have expressed concern that TSWG's approach results in recommendations that are too conservative. Please address that concern. In particular, how will you ensure that break-through technologies are adopted when appropriate?

Answer S&T 2.d. The **Technical Support Working Group (TSWG)** is an interagency national forum that identifies, prioritizes, and coordinates interagency and international research and development (R&D) requirements for combating terrorism. The Department of State exercises oversight.

On June 4, 2003, DHS issued a $33M procurement request to TSWG to "solicit commercial-off-the-shelf technologies for use by federal, state, and local entities, providing the technical clearing house function. . ., and to upgrade its infrastructure to perform this function.

The TSWG rapidly develops technologies and equipment to meet the high-priority needs of the combating terrorism community.

On May 14, 2003 TSWG and DHS issued a joint Broad Agency Announcement seeking technology for fifty top priority requirements. TSWG received 3,344 responses to this call. From these responses, TSWG requested 223 proposers to submit White Papers. Based on the evaluation of these White Papers, TSWG requested and received 47 full proposals. TSWG has completed these evaluations and is now in the contracts negotiation process. TSWG has also supported DHS S&T by providing technical evaluation of unsolicited proposals. DHS has provided an additional $30M in fiscal year 2004 to fund the most meritorious of these submissions.

DHS has not made final decisions on how to implement the clearinghouse functions. Until firm decisions can be made, and staff gathered to support them, the clearinghouse function required in Section 313 is being satisfied in two ways; funding of Public Safety and Security Institute for Technology (PSITEC) ($10M in fiscal

year 2004) to perform the clearinghouse function and the DHS working relationship with the Technology Support Working Group. PSITEC develops knowledge-based services that provide access to, and distribution of, information and services relevant to public safety technologies. PSITEC will serve as the clearinghouse—a single point of entry—for the public safety and first responder community, providing access to relevant information on technologies and products, test and evaluation, as well as engaging in projects of interest and importance to them.

HSARPA has a single focus and a single funding source for its research. Its staff is experienced; its research goals are stressing. The planned research will press the state of the art and about $13M of the fiscal year 2004 HSARPA budget is targeted specifically to nurture break-through research on the most difficult homeland security problems. Although true break-through technologies are rare, HSARPA's organization, plans, budgets and assigned functions ensure that if one emerges, it will be developed and moved quickly to field use.

e. Homeland Security Institute (HSI)
- **Has the HSI been established?**
- **If so, how many people are employed there?**
- **Who is leading the Institute?**
- **What is its budget for the current fiscal year?**
- **What tasks and responsibilities has the Secretary assigned to the Institute?**
- **What products or results has the Institute reported?**
- **If it has not been established, when does the Department expect to establish it?**

Answer S&T 2.e. The Homeland Security Institute will be established in fiscal year 2004. In early December 2003 the Science and Technology Directorate released a Request for Proposals to establish the Institute as as a federally funded research and development center (FFRDC) to provide analytic support for the Department. Proposals were due January 28, 2004, with award projected on May 1, 2004. The budget is expected to be $128M over 5 years ($8.5M in fiscal year 2004, approximately $30M per year fiscal year 2005–fiscal year 2008). The Homeland Security Institute will provide a wide range research, studies, analyses, analytic and computational models, simulations, and other technical and analytical support useful for policy and program planning, and management by the Department. Core competency areas include: systems evaluations, technology assessments, operational assessments, resource and support analyses, analyses supporting the SAFETY Act, and field operations analyses.

f. Establishment/Contract with a Federally Funded Research & Development Center (FFRDC)
- **What steps has the S&T Directorate taken, to date, to contract with or establish an FFRDC?**
- **If no selections have been made, please describe the process and selection criteria that the Department will use to make any selections.**

Answer S&T 2.f. addition to information provided in response 2.e. selection criteria identified in the Request for Proposals included Management and Technical Approach, Past Performance and Past Experience, Subcontracting, and Cost and Financial Capability.

g. University–Based Centers for Homeland Security
- **How many university-based centers does the S&T Directorate expect to establish?**
- **What criteria will the Directorate use in establishing such Centers?**
- **What types of research work does the Directorate intend to assign to such Centers?**

Answer S&T 2.g. On November 25, 2003, the Department announced selection of the University of Southern California as the first Homeland Security Center, for Risk and Economic Analysis of Terrorism Events. The Center will develop modeling capabilities that cut across general threats against critical infrastructure targets, such as electrical power, transportation and telecommunications. The Center will also develop tools for emergency response planning. Center staff recently met with S&T officials and portfolio managers to begin detailed dialogue on a work plan to guide the Center's research. The Center has assembled a team of experts across the country, to include partnerships with the University of California at Berkeley; the University of Wisconsin-Madison's Center for Human Performance and Analysis; Structured Decision Corporation; and New York University's Institute for Civil Infrastructure Systems.

Our objective is to create additional Centers, each focusing on a different area important to homeland security, including social sciences, psychology, and life sciences as well as engineering and physical sciences. These Centers will be mission-focused and targeted to research areas that leverage the multidisciplinary capabilities of universities. We are pleased to have the support of the National Academies of Science, which has agreed to convene two workshops to solicit university community and scientific expertise input on a forward-leaning agenda for the Centers of Excellence program. The NAS held the first workshop on the research agenda last month (January 2004) and will hold its second workshop on the education agenda in April 2004.

Our intent is to manage solicitation processes and announce awards for two additional Centers of Excellence this year. On December 12, 2003, DHS released a Broad Agency Announcement (BAA) in the area of agricultural biosecurity. Through this BAA, we will fund two Centers of Excellence, one dedicated to education and research of foreign animal and high-consequence zoonotic diseases; and a second Center dedicated to post-harvest food security.

h. Headquarters Laboratory Section 309 of the Homeland Security Act gives the Secretary authority to contract with or enter into joint sponsorship agreements with a DOE laboratory.

• Has the Secretary established a headquarters laboratory, in accordance with section 308 of the Homeland Security Act?

• If so, where is it, who is running it, how many people are working there, what is the funding for the current fiscal year, and what functions does it perform?

• If it has not been established, will the Department do so? If so, when?

Answer S&T 2.h. No, the Department of Homeland Security has not established a headquarters laboratory. The S&T Directorate is accessing the capability base of the national laboratories in accordance with DHS mission requirements for the intramural and extramural programs. The DOE national laboratories, sites, and technology centers have a tremendous breadth of technical expertise and capability in areas related to homeland security. The DHS/S&T is committed to maximizing the opportunities for all of the DOE assets to play a role in supporting the missions of the Department.

i. Federal Clearinghouse

• Has the Secretary established a federal clearinghouse for dissemination of homeland security technology information? If not, when will it be established?

• Where is it?

• Who is running it?

• What is its telephone number?

• What is its budget for this fiscal year?

Answer S&T 2.i. DHS has responsibility for the clearinghouse function. However, it has not been "established" as a separate entity within the S&T Directorate to date. Currently, the clearinghouse functions required in Section 313 of the establishing legislation are being satisfied in two primary ways.

First, on June 4, 2003, DHS established a working relationship with the Technology Support Working Group by providing funding ($33M in fiscal year 2003 and $30M in fiscal year 2004) to "solicit commercial-off-the-shelf technologies for use by federal, state, and local entities, providing the technical clearing house function. . ., and to upgrade its infrastructure to perform this extra work.

Second, in fiscal year 2004, DHS will fund the Public Safety and Security Institute for Technology (PSITEC) ($10M in fiscal year 2004) to perform the clearinghouse function.

PSITEC develops knowledge-based services that provide access to, and distribution of, information and services relevant to public safety technologies. PSITEC will serve as the clearinghouse—a single point of entry—for the public safety and first responder community, providing access to relevant information on technologies and products, test and evaluation, as well as engaging in projects of interest and importance to them.

For the longer term, DHS is considering a range of possible solutions for carrying out the "centralized Federal clearinghouse" function. Some appear more cost effective than establishment of a separate, stand-alone clearinghouse. Until decisions can be made based on experience, these two methods together with other activities such as information provided on the public website, issuing Federal Funding Opportunities for technologies and research (with explicit information on research topics and submission procedures), and writing standards to evaluate technologies, constitute the clearinghouse function.

The clearinghouse function as described above resides in the S&T Directorate of DHS. Pending the establishment of a single centralized Federal clearinghouse, the Points of Contact information listed on the public webpage (as described above) should be used.

The clearing house function has no separable budget. DHS has provided a total of $63M to TSWG, a small portion of which covers clearinghouse functions. In fiscal year 2004, $10M will be used to support PSITECH and its functions.

3. Standards

a. Your statement to the Subcommittee describes development and implementation of standards as a key area of emphasis for the Directorate, and you have recently signed a Memorandum of Understanding (MOU) with the National Institute of Standards and Technology to facilitate that.

- **Please provide the Subcommittee with a copy of the signed MOU.**
- **What are the responsibilities of the Science and Technology Directorate for homeland security standards, and what responsibilities lie elsewhere within the Department and other federal agencies?**

Answer S&T 3.a. The MOU with the National Institute of Standards and Technology is included as Appendix D.

Standards are an integral component of the mission of the S&T Directorate because they provide the objective measures of homeland security systems effectiveness. Standards are a fundamental component of the cradle to grave research, development, test, evaluation and transition to service product cycle. Thus, standards for homeland security applications must be constructed in parallel with the defensive systems to establish minimum criteria for effectiveness that encompass: basic functionality, adequacy for the task, interoperability, efficiency, and sustainability. Standards development requires a detailed knowledge of the technical attributes and capabilities of the system and a comprehensive understanding of the user requirements and operating conditions. A tight coupling must be maintained between the operational users, standards, and all the technologies that comprise the system at each step in the research, development, test and evaluation process.

During the transition phase of the Department, the need for standards to address design, procurement, deployment, and use of the radiological and biological detectors was determined to be a key need. In collaboration with the National Institute of Standards and Technology (NIST), the American National Standards Institute (ANSI) and the Institute of Electrical and Electronic Engineers (IEEE), the DHS S&T transition team began development of standards for four high-priority classes of radiation detection equipment. The four classes are personal dosimeters ("pagers"), alarming hand-held detectors, hand-held isotope identifiers, and radiation portals. These standards have been released in draft form and will soon go to ballot, in accordance with ANSI process requirements for national consensus standards. A contract to develop a standard test method for hand-held bulk anthrax immunoassay kits has been negotiated with the private sector group AOAC International. A Task Force set up under this contract has developed a plan of work to validate these test kits at Dugway Proving Grounds, Utah.

Work is also progressing in the areas of training standards and personnel certification. Additional standards needs for both detection and response are being identified as part of a systematic evaluation of capabilities versus needs for standards to support the homeland security mission related equipment, operators, models and analyses, data and information, and integrated systems.

In addition, the S&T Directorate has been working with the Oklahoma City Memorial Institute for Preventing Terrorism (MIPT) to deploy a web-based tool that will communicate directly with user communities. The user community has had a broad representation in the development of the tool. "Project Responder," with direct input from DHS, is evolving into a tool that can catalog technologies, provide links to manufacturer data, and indicate which standards apply and also the degree of compliance with DHS standards. It will also show links to appropriate training and with potential grant programs.

In all of these standards projects, the S&T Directorate coordinates with the customers in the operational directorates and with experts in other federal agencies including DOE, DOD, HHS, EPA, FDA, USDA and others.

b. Are your efforts focused only on technical standards for equipment, or do they include other things such as preparedness and cyber security standards?

Answer S&T 3.b. S&T Standards are not limited to technical standards. They will also include standards for Information Technology (IT) products and services that are needed by the operational directorates. These include cyber security standards, as well as standards for biometric identification technologies, "smart cards", and ra-

diofrequency ID cards (RFID) for baggage identification. The standards process also involves developing tools for accreditation of laboratories for Test and Evaluation (T&E) for technical products and services as well as IT products and services.

c. How are you engaging the private sector, including standards-setting organizations, in these efforts?
Answer S&T 3.c. A number of Standards Development Organizations (SDOs) have stepped forward to offer their help to the S&T Directorate in development of consensus standards for Homeland Security. The American National Standards Institute (ANSI) has volunteered to coordinate the activities of about 280 SDOs that are members of ANSI as well as other SDOs to be identified in development of standards under the auspices of the Homeland Security Standards Panel. Other SDOs are establishing their own Homeland Security committees and engaging DHS directly in their planning processes. Four of the many important private sector groups are: the National Fire Protection Association (NFPA), American Society for Testing and Materials (ASTM), the Institute for Electrical and Electronics Engineers (IEEE), and The Infrastructure Security Partnership (TISP). Each of these groups draws heavily from private sector volunteers in establishing committees and standards writing groups.

d. The American National Standards Institute (ANSI) recently announced a charter for its Homeland Security Standards Panel. It cited ten priority standards needs identified by DHS. Is that list an accurate description of the Directorate's priorities in this area?
Answer S&T 3.d. The ANSI Homeland Security Standards Panel (HSSP) has held a number of meetings of an Interim Steering Committee with DHS S&T staff and one full meeting of the HSSP on June 9 and 10, 2003. The ten areas identified on the HSSP web site (posted in May 2003) are those where it was judged that the HSSP could provide useful coordination in the early stages of establishing writing groups. Progress is being made in these 10 areas. However, there are other areas, including standards needed for public health, which were not on the initial list because ANSI had yet to identify the SDOs who could contribute in the near term. In such cases, DHS is working directly with other SDOs.

• **How will the Directorate be working with ANSI in the development of these and other standards?**
Answer S&T 3.d. Bullet 1. Under the charter of the HSSP, ANSI does not develop standards. Rather they identify a member SDO (IEEE, for example) to develop a consensus standard for a given technical application. The SDO then coordinates directly with S&T Directorate in preparing a scope of work for the new standard. The writing group for the standard typically includes representatives from DHS, other federal state and local agencies as well as private sector users and manufacturers. The HSSP recognizes the need to involve representatives of emergency responders on these writing groups as appropriate. As a recent example of this process, the IEEE is preparing a suite of four standards for radiation detectors for emergency responders under an N42 subcommittee. Writing group members came from the private sector, from state and local agencies as wells as the DOE national labs, the National Institute of Standards and Technology (NIST) and several other federal agencies. The standards will be published as ANSI standards in the United States. A similar activity is underway to develop standard methods for detection of anthrax spores working with the Association of Analytical Chemists (AOAC International).

• **Are there any areas where an approach other than voluntary consensus will be needed? If so, what are they and how will you proceed?**
Answer S&T 3.d. Bullet 2. Under the National Technology Transfer Act, DHS will use consensus standards to the full extent possible. Exceptions to the use of voluntary consensus standards will arise in development of Test and Evaluation (T&E) protocols for detectors used for CBRNE agents (chemical, biological, radiological, nuclear and explosives). The writing groups preparing these protocols will require access to sensitive information that cannot be shared with the usual volunteer committee. The S&T Directorate is supporting working groups now at the federal and national labs and appropriate levels of clearance are required to participate in these efforts. Standards for other protective measures may also contain sensitive information and participation on the writing groups will be limited as required by security considerations.

• **Will any of these standards require the participation of international organizations, such as the International Standards Organization (ISO), the International Electrotechnical Commission (IEC), and the International**

Telecommunications Union Standardization Department (ITU)? If so, how will you work with them?

Answer S&T 3.d. Bullet 3. The answer is yes: all of these international standards organizations will be engaged. And, two others should be mentioned: the International Atomic Energy Agency (IAEA), and the International Committee on Information Technology Standards (INCITS). One of the near term goals of the ANSI HSSP is to plan a workshop on international standards for homeland security that will allow the national committees to coordinate with the appropriate international counterpart. Much of this coordination is already underway with ISO, IEC, IAEA and INCITS. The US private sector has a very strong multinational component, and manufacturers want to have common standards for their products for their US and overseas markets. With appropriate coordination we expect that many American National Standards will be adopted internationally by one of the umbrella organizations.

4. Funding for the S&T Directorate—The Directorate of Science and Technology requests $804 million for research and development (R&D) efforts for next fiscal year, representing a 43 percent increase over current year levels. However, even after accounting for such an increase, the Directorate's funding level for its science and technology programs is only two percent of the overall request for the Department of Homeland Security for fiscal year 2004. Other government agencies that engage in research programs, as well as private sector firms, try to budget upwards of ten percent or more of their total budget for their R&D work.

a. Is the Directorate's budget request for fiscal year 2004 adequate to address all of the S&T needs of the Department?

b. What, if any, key shortfalls exist (such as R&D work regarding cyber security)?

Answer S&T 4.a. The Science and Technology Directorate has reviewed its authorized fiscal year 2004 funding and its proposed fiscal year 2005 funding and presently believes the current and proposed funding is adequate. However, we continue to assess our research and development plans. If we determine that the proposed amount of our funding is not sufficient to meet requirements, we would bring that information forward for consideration through the appropriate mechanisms. Additionally, in order to accurately determine what level of funding is needed for our research, development, testing and evaluation (RDT&E) activities, we will continue to work with other agencies with R&D responsibilities to identify requirements and gaps in funding. This coordinated approach will assist in making the right investments while preventing unnecessary and wasteful duplication.

Answer S&T 4.b. The Science and Technology Directorate is currently in the process of identifying and reviewing all relevant homeland security documentation to determine the requirements for research and development. If we identify needs that are not currently being addressed, we will bring that information forward through the appropriate mechanisms.

5. Time lines Please provide the subcommittee with time lines for specific steps the Directorate is taking to implement the following:

a. The Homeland Security Advanced Research Projects Agency

b. University–Based Centers for Homeland Security

c. The Homeland Security Institute

d. The Technology Clearinghouse and the Homeland Security Science and Technology Advisory Committee

(The time lines should include expected dates of naming and hiring key personnel, program staffing, solicitations, decisions, awards, acquisitions and procurement, and other key milestones.)

Answer S&T 5.a. HSARPA was established in March of 2003 when the Department was stood up.

Answer S&T 5.b. In fiscal year 2004, S&T 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 aid in the protection of our nation's critical infrastructure and provide tools to improve operational planning for emergency response. 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. These proposals were due on February 9, 2004, and are currently under review.

Answer S&T 5.c. A formal solicitation was issued in December 2003 for the Homeland Security Institute, a legislative requirement for a federally funded research

and development center to assist the Secretary and the Department in addressing important homeland security issues that require scientific, technical, and analytical expertise. Proposals were received in January 2004. Those proposals are currently being evaluated with an expected five-year award by early May 2004.

Answer S&T 5.d. Technology Clearinghouse: DHS has responsibility for the clearinghouse function. However, it has not been "established" as a separate entity within the S&T Directorate to date. Currently, the clearinghouse functions required in Section 313 of the establishing legislation are being satisfied in two primary ways.

First, on June 4, 2003, DHS established a working relationship with the Technology Support Working Group by providing funding ($33M in fiscal year 2003 and $30M in fiscal year 2004) to "solicit commercial-off-the-shelf technologies for use by federal, state, and local entities, providing the technical clearing house function. . . ", and to upgrade its infrastructure to perform this extra work.

Second, in fiscal year 2004, DHS will fund the Public Safety and Security Institute for Technology (PSITEC) ($10M in fiscal year 2004) to perform the clearinghouse function.

PSITEC develops knowledge-based services that provide access to, and distribution of, information and services relevant to public safety technologies. PSITEC will serve as the clearinghouse—a single point of entry—for the public safety and first responder community, providing access to relevant information on technologies and products, test and evaluation, as well as engaging in projects of interest and importance to them.

For the longer term, DHS is considering a range of possible solutions for carrying out the "centralized Federal clearinghouse" function. Some appear more cost effective than establishment of a separate, stand-alone clearinghouse. Until decisions can be made based on experience, these two methods together with other activities such as information provided on the public website, issuing Federal Funding Opportunities for technologies and research (with explicit information on research topics and submission procedures), and writing standards to evaluate technologies, constitute the clearinghouse function.

The clearinghouse function as described above resides in the S&T Directorate of DHS.

Pending the establishment of a single centralized Federal clearinghouse, the Points of Contact information listed on the public webpage (as described above) should be used.

HS S&T Advisory Committee: S&T has now established the Homeland Security Science and Technology Advisory Committee, a legislative requirement for an advisory committee to be a source of independent, scientific and technical planning advice for the Under Secretary for Science and Technology. The committee will hold its initial meeting in February 2004.

6. Outsourcing IT work—Has the Department, and the S&T Directorate specifically, investigated any national security considerations to the outsourcing of IT work by American firms to foreign companies and the potential impact to the security of U.S. critical infrastructure that is owned and operated by the American firms? If so, what are the concerns of the Department?

Answer S&T 6. The S&T Directorate has not specifically investigated any national security concerns related to the outsourcing of IT work by American firms to foreign companies and the potential impacts to the security of U.S. critical infrastructure that is owned and operated by the American firms.

7. First Responder

a. What are the major science and technology issues that the Department of Homeland Security has identified to support communications needs for first responders, evacuation centers, emergency command centers, and other critical rescue operations at the scene of a disaster and at nearby hospitals, and other components of the emergency response network? What actions is the Science and Technology Directorate taking to address these needs?

Answer S&T 7.a. To enhance public safety communications and interoperability, the Department of Homeland Security's (DHS) Science and Technology Directorate (S&T), through the efforts of the SAFECOM Program, is addressing the key public safety communication needs for technology solutions, technology assistance and outreach, standards, federal coordination, and policy direction.

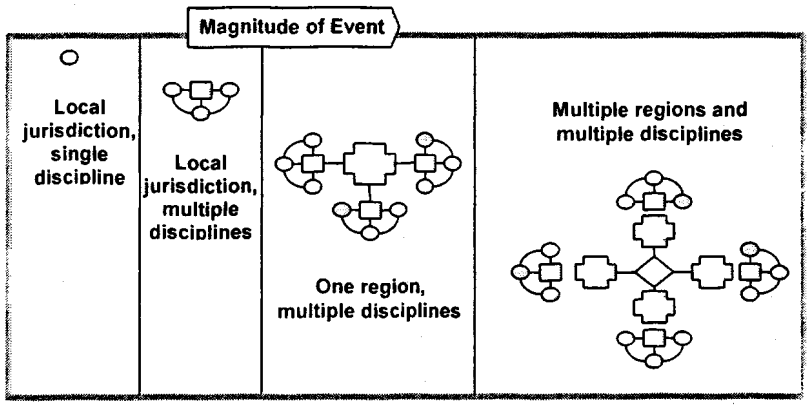
b. Describe the goals and objectives of Project SAFECOM and the nature and extent of the Department's involvement in it. What type of system ar-

chitecture does the Department envision will be needed for a first responder communications system?

Answer S&T 7.b. Several government programs have done a good deal of work on this issue; unfortunately, much of it has been disconnected, fragmented, and, at times, at odds with larger goals. In an effort to coordinate the various Federal initiatives, SAFECOM was established by the Office of Management and Budget (OMB) and approved by the President's Management Council (PMC) as a high priority electronic government (E-gov) initiative. The mission of SAFECOM is to enable public safety nationwide (across local, tribal, State and Federal organizations) to improve public safety response through more effective and efficient interoperable communications. By definition, communications interoperability refers to the ability of public safety agencies to talk across disciplines and jurisdictions via radio communications systems—to exchange voice, data and/or video with one another on demand, in real time, when needed. To this end, SAFECOM recognizes that before interoperability can occur, reliable, mission-critical, agency-specific communications are first necessary for public safety agencies. SAFECOM subsequently is addressing the intricately related issues of public safety communications and communications interoperability.

By leveraging the knowledge and expertise of the public safety community and through examining other programs and studies addressing this same issue, SAFECOM has saved time and money in identifying key issues, needs, and existing efforts. The efforts of the Federal Emergency Management Agency (FEMA) to identify these leaders of the public safety community, engage them in a strategic dialogue, and establish the governance structure for SAFECOM have enabled the program to efficiently grasp the depth of issues associated with public safety communications. However, it became clear that in order to address many of the problems, a technical capacity would be necessary to deal with issues such as spectrum, standards, and the development and incorporation of emerging communications technologies. As DHS stood up, S&T became an obvious home for SAFECOM. At S&T, SAFECOM is building off of the work of FEMA and developing both short- and long-term strategies to address immediate public safety communication needs while creating a migration strategy toward more spectrally efficient systems.

SAFECOM's long-term vision of the public safety communications architecture is a national "system of systems" that adapts to an incident, as illustrated below.



c. Wireless Communications

- **What science and technology requirements have you identified with respect to network architecture and security, equipment and software, frequencies used for wireless communications, system redundancy and back-up, participation of the appropriate federal agencies, authentication of participants (credentialing), the use of developing technologies such as artificial intelligence and database mining, and standards?**

Answer S&T 7.c. Bullet 1. SAFECOM is currently supporting the development of a comprehensive statement of requirements for public safety communications. This SoR will provide SAFECOM with an assessment of functional needs that public safety has in order to communicate, both via voice and data. Additionally, through its coordination with projects such as Disaster Management and the Capital Wireless Integrated Network (CapWIN), SAFECOM is addressing issues related to: how best to structure wireless networks so they interface well with existing wired architectures; identification of what equipment is needed, where more capacity (including redundancy) is needed; how to link all participating Federal, State, and local agencies; and the identification of ways in which to authenticate network users and apply encryption. Because the wireless world includes increasing use of technologies such as voice over IP and remote database management and data mining, SAFECOM will continue to address standards to ensure integration of public safety wired and wireless solutions. No potentially useful technology is being overlooked or will be excluded from consideration, either as a commercial off the shelf (COTS) solution, or for R&D.

- Are there any efforts underway to develop an override capacity for the cell phones of key emergency personnel and local officials to ensure that they can communicate with one another in the event of an emergency? Is the S&T Directorate involved in the Wireless Priority Program? If so, how?

Answer S&T 7.c. Bullet 2. The National Communications System (NCS), which is part of DHS, was instructed in January 1995 to work with industry and Government to implement a wireless priority service for national security and emergency preparedness workers. To this end, the Priority Services (PS) group of NCS conducts technical analyses and research and development focused on identifying wireless and Internet priority service solutions to overcome blockage in cellular systems when availability is most critical. SAFECOM has met with NCS representatives to discuss areas of coordination, and more importantly, to begin examining the relationship between priority cellular services and public safety owned land mobile radio systems (LMRS). Understanding the intricacies of relating cellular services to LMRS is important since LMRS provides first responders and broader public safety community with their mission-critical communications. As wide spread as cellular services are, the infrastructure is yet not adequate to support crucial public safety communication needs. The National Task Force on Interoperability report released in February 2003 offers an explanation as to why public safety cannot currently rely on commercial services for emergency communications.

Although public safety personnel regularly use cellular phones, personal digital assistants (PDAs), and other commercial wireless devices and services, these devices are currently not well suited for public safety mission-critical communications during critical incidents. Public safety officials cannot depend on commercial systems that can be overloaded and unavailable. Experience has shown such systems are often the most unreliable during critical incidents when public demand overwhelms the system. Public safety officials have unique and demanding communications requirements. Optimal public safety radio communication systems require

- Dedicated channels and priority access that is available at all times to handle unexpected emergencies.
- Reliable one-to-many broadcast capability, a feature not generally available in cellular systems.
- Highly reliable and redundant networks that are engineered and maintained to withstand natural disasters and other emergencies.
- The best possible coverage within a given geographic area, with a minimum of dead zones.
- And, unique equipment designed for quick response in emergency situations—dialing, waiting for call connection, and busy signals are unacceptable during critical events when seconds can mean the difference between life and death.[1]

SAFECOM looks forward to continued coordination and work with NCS with respect to providing input on the communication issues and needs of public safety.

[1] *"Why Can"t We Talk? Working Together to Bridge the Communications Gap To Save Lives: A Guide for Public Officials," The National Task Force on Interoperability, February 2003, page 11.*

d. How will the S&T Directorate's work regarding the testing and evaluation of first responder equipment relate to similar work to be carried out by the Office of Domestic Preparedness? Does the Department plan on continuing this division of labor between the two Department of Homeland Security organizations?

Answer S&T 7.d. The primary focus of the ODP program has been on Personal Protective Equipment (PPE) for emergency responders. The S&T Directorate is responsible for the science and technology and testing and evaluation (T&E) of all equipment, products, services and systems needed for a national program in homeland security. The T&E activity needs to be performed as one component of equipment development. This includes identification of the need, development of performance specifications, testing and evaluation by accredited testing laboratories, and certification. The DHS system to certify equipment for emergency responders should take full advantage of this infrastructure for measurements, standards and certification being developed by the S&T Directorate. The S&T Directorate has in fiscal year 2003 launched major efforts to develop detector standards for emergency responders for radiological/nuclear and biological agents. The S&T Directorate is coordinating on development of S&T standards with NIOSH, NIST/Office of Law Enforcement Standards (OLES) and SBCCOM (Army) personnel who are the performers for the ODP sponsored work. The technical direction for this work in fiscal year 2004 should reside in the S&T Directorate to ensure that consistent and complete standards are developed for homeland security applications for emergency responders.

e. What types of standards will be developed for state and local first responders? What types and categories of equipment will standards be developed for? When will such standards be developed? How will the Department communicate its decisions to state and local governments?

Answer S&T 7.e. There are several ways to categorize standards for emergency responders. The needs that have been identified to date can be put into categories such as CBRNE threat agents used in three phases of a terrorist attack: detect/prevent, response/recovery, and mitigation/decontamination. State and local first responders are most interested in the instruments and detectors used in the early stages. Other cross cutting projects that require standards include: communications hardware and software, certification (of products, service and personnel), personal protective equipment (PPE), and training. Working groups are being established to look at standards requirements in each of these areas. The radiation detector standards, developed on a fast track, will be available in 2003. The standards for immunoassay kits for anthrax detection will be available in 2004. The DHS Office for State and Local will be apprised on the state of development of standards and will serve as a conduit to the state and local emergency planners. In addition, almost all the standards writing groups will have participants for national groups that coordinate at the state and local level.

f. What steps are being taken by the S&T Directorate to upgrade biohazard detection technology so that first responders and health care workers can know the threat they face? Please outline any specific actions that have been initiated by the Department and when they will be completed.

Answer S&T 7.f. The S&T Directorate has partnered with the Office of the Secretary of Defense (DOD) to fund AOAC International to develop reference methods for detection of anthrax using immunoassay kits. These kits are widely used by emergency responders for qualitative testing of suspicious powders and at present there is no guidance to purchasing agents for first responders and health care workers on the performance specifications for these detectors. The contract with AOAC called for establishment of a Task Force to identify a reference method, a reference laboratory and a protocol for testing commercial products to an agreed standard. This Task Force is co-chaired by scientists from the Office of Science and Technology Policy (OSTP) and the DHS S&T Directorate, and includes representatives from DOD, CDC, USDA, FDA as well as private sector manufacturers and representatives from state and local user groups. After two meetings this summer the Task Force has recommended a draft protocol and authorized tests by the reference laboratory at the Army's Dugway Proving Grounds in Utah. Upon completion of initial testing by the reference laboratory, a round of multilab measurements will take place in Winter 2003–2004 and validation of the commercial kits is expected in May 2004. First responders and health care workers will then have the assurance that these immunoassay kits can be used as one component of their detection and prevention strategy.

8. Intelligence Input for S&T—What types of intelligence is the S&T Directorate regularly receiving on threats to the homeland, which can inform priorities for research and development work? What relationships has the S&T Directorate established with the Information Analysis and Infrastructure Protection Directorate and other elements of the Intelligence Community?

Answer S&T 8. The S&T Directorate is receiving current threat and vulnerability information through the Information Analysis and Infrastructure Protection Directorate. Members of our staff engage in intelligence community activities related to science and technology, and a number of our staff participate in interagency working groups that are addressing the various threats. Staff from our Threat and Vulnerability, Testing and Assessment portfolio and the Critical Infrastructure Protection portfolio regularly interact with staff from the IAIP Directorate. In addition, we have established an Office of Comparative Studies to provide threat and vulnerability assessments with the aid of IAIP.

9. Biodefense

a. In your statement before the Subcommittee, you indicate that $365 million is requested for fiscal year 04 for biological countermeasures, specifically for the National Biodefense Analysis and Countermeasures Center (NBACC) and for a Biological Warning and Incident Characterization System (BWIC). Please provide the Subcommittee with a breakdown of fiscal year 03 funding and the fiscal year 04 request for those two programs and other activities in this area of emphasis, including funding you expect to administer through HSARPA.

Answer S&T 9.a.

Our fiscal year 2004 Appropriation was $286.5M of which $88M is directed to NBACC construction. Fiscal year 2004 execution plans in the above areas allocated as follows:

NBACC—
R&D program—$60M
Construction—$88M
Biological Warning and Incident Characterization Integration- $4.1M* *includes use of authorized carryover from fiscal year 2003

Fiscal year 2005 President's Budget is allocated as follows:

NBACC—
R&D program—$65M
Construction—$35M
Biological Warning and Incident Characterization Integration - $9M

b. How do the bioterrorism R&D activities in the Directorate differ from the Department of Health and Human Services and the Department of Defense efforts? What specific mechanisms is the Directorate using to coordinate bioterrorism R&D with these other agencies (including the collaboration required by § 304 of the Homeland Security Act) and with the Environmental Protection Agency?

Answer S&T 9.b. The Directorate's bioterrorism R&D activities focus on the development of domestic biological countermeasures for deterrence, detection, and mitigation of potential biological attacks on the nations population, infrastructure and agriculture. Priorities are focused on countermeasures against catastrophic events including large scale anthrax or small pox attacks, and a foot and mouth disease in cattle. The Department of Defense bioterrorism R&D efforts focus on force protection and readiness with a concept of operations that support detection thresholds and decontamination not directly applicable to civilian requirements. Military doctrine views chemical/biological threat more as an area denial weapon that mobility can counter. This does not apply to the domestic situation and potential scenarios where mobility is not a major factor for large populations. The Department of Health and Human Services is focused more on health and medical applications such as clinical diagnostics, therapeutics, and vaccines. For example, fundamental research includes the study of pathogencity mechanisms and host response associated with a specific agent. The Environmental Protection Agency has programs in water security and decontamination. The Directorate's Biological & Chemical Countermeasures Portfolio works closely with the DOD Joint Program Office for Chemical and Biological Defense, the Defense Threat Reduction Agency, Joint Requirements Office and the Office of the Assistant to the Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs to leverage activities and minimize overlapping efforts. For example, a program is underway to develop a national template for a joint military and civilian consequence management response following urban detection of an aerosolized biothreat agent. The Directorate also has liaisons that

work with DHHS CDC and NIH to identify areas of common interest to maximize resource allocation. The Directorate identifies NIH research deliverables that will apply to assay development, bioforensics, and detection technologies. The Directorate also works closely with the EPA to understand how the water security and restoration efforts contribute to the overall national biodefense system.

c. Please describe how the National Bio–Weapons Defense Analysis Center is being established.

(1.) Is this entity the same as the National Biodefense Analysis and Countermeasures Center described in the Department's fiscal year 2004 budget request?

(2.) What will be the role of other agencies in administering this Center?

(3.) Who will set its priorities?

(4.) Please provide a detailed description of BWIC, including:

• How you decided that this system should be a priority compared to investment in other needs such as cybersecurity or radiological countermeasures?

• How you decided what its components should be?

• What issues and hurdles you need to overcome to develop and deploy this system and make it "seamless," and how you intend to overcome them?

• How you will develop and deploy the system, including how you will involve other government agencies, industry, and academic research centers?

Answer S&T 9.c. The fully integrated, biological warning and incident characterization (BWIC) system enables timely warning and response in the event of a biological attack. The system combines information from Biosurveillance and environmental monitoring systems with key modeling tools and databases to asses the extent of the attack, extent of area contaminated and exposed and affected population. BWIC will provide decision makers with a better understanding of the scale of the event and allow rapid formulation and implementation of appropriate responses, including phasing of critical resources. Through discussions with the Homeland Security Council, Office of the Vice President, and Office of Science and Technology Policy, it was established that the BWIC system will be instrumental in the success of an overall national biodefense posture and thus, a high priority for the Directorate's R&D efforts. Because there are many agency participants, some of which have programs underway that will need to provide data for BWIC, coordination is essential for success. Through the development of an interagency steering committee, which will include an avenue for local user input, each respective agency will develop the path forward and timeline together to ensure the resulting BWIC system will meet the consensus requirements. The system will be systematically linked with existing biomonitoring networks (BioWatch, USPS) and CDC's biosurveillance system. BWIC will be compatible with CEC, local, regional, and national emergency operation centers, and the Homeland Security Operation Center and incorporate plume model/hazard and epidemiological prediction codes for use as a public health response tool. Federal, State, and local government agencies and, through appropriate extramural R&D competitive mechanisms, industry and academia will be involved in many of the critical steps for successful BWIC development and deployment.

10. Cybersecurity R&D

a. How is the Directorate managing R&D with respect to cybersecurity?

Answer S&T 10.a. The Science and Technology Directorate's Cybersecurity Portfolio Manager sets long-term strategies and the planning and budgeting to accomplish those strategies. Work is conducted through either the Homeland Security Advanced Research Projects Agency or the Office of Research and Development. This entire process is guided by the needs and requirements of our customers.

b. Does the S&T Directorate intend to support a single official to oversee its cyber security programs? If so, where, organizationally, will it be located, and what principal duties will be assigned to it? How will it relate to cyber security work within the Information Analysis and Infrastructure Protection Directorate? In light of the fact that the Critical Infrastructure Board no longer exists, is the S&T Directorate adequately resourced consistent with its new cyber security responsibilities?

Answer S&T 10.b. The Science and Technology Directorate designates a single manager to be responsible for the cyber security work conducted by the S&T Directorate. This individual is a member of the management team of the Threat and Vul-

nerability, Testing and Assessment Portfolio. The work the S&T Directorate conducts in cyber security is closely coordinated with the Information Analysis and Infrastructure Protection Directorate so that the work is complimentary, not duplicative. The S&T Directorate is adequately resourced to conduct the cyber security work for which it is responsible.

c. Your statement lists cybersecurity as one activity in the Threat and Vulnerability, Testing and Assessment portfolio, for which the total fiscal year 04 budget request is $90 million. What specific kinds of R&D activities are being undertaken in cybersecurity, and what are the current and requested levels of funding for them? How were those priorities identified?
Answer S&T 10.c. The Cyber Security Funding Portfolio is funded at a level of $18M in fiscal year 2004, and has a request of $18M for fiscal year 2005. The Portfolio is currently divided into six programs. Five of these programs have budgets ranging from $1M to almost $5M. These programs focus on (1) next-generation cyber security technologies, (2) cyber security infrastructure technology (the application of more generic technologies, such as modeling, simulation, visualization, to support and facilitate the development, deployment or management of cyber security technologies), (3) small (high impact, low cost) development projects, (4) technical research studies, and (5) cooperative communities, which involves pilot projects, fostering public-private partnerships, community building and workshops. The sixth program is the Small Business Innovation Research (SBIR) component of the S&T budget, for which $450k (2.5% of the portfolio's funding) has been set aside. In addition to the programs described above, a contract has been awarded for technical support for the Cyber Security Research and Development Center. This "virtual" Center is the umbrella under which DHS-funded cyber security R&D activities will be performed. The technical support contract for the center is focused on supporting S&T in executing its cyber security R&D programs, and on supporting the Department's emphasis on public-private partnerships through interactions with university and industry research groups, cyber security product and service vendors, and the venture capital community.

Some of the priorities that are currently being addressed in the Cyber Security R&D Portfolio include (but are not limited to):

- Infrastructural issues associated with securing protocols that underlie the Internet—work focused on Secure Domain Name System (DNSSEC) and Secure Border Gateway Protocol (Secure BGP);
- Development of large scale data sets to facilitate cyber security testing and to enable the development of the kinds of evaluations that can lead to metrics for cyber security;
- Co-funding with the National Science Foundation of two large multi-university collaborative efforts: a large scale testbed and a cyber security testing framework;
- Critical infrastructure-specific cyber security needs, including coordination of R&D on supervisory control and data acquisition (SCADA) systems with DHS's Critical Infrastructure Protection Portfolio, as well as collaboration with the Department of Treasury to focus on Banking and Finance Sector needs;
- Research focused on DHS internal customer needs, such as Internet Priority Services.

These priorities were derived from a wide variety of sources. These include:

- Written policy documents (such as the National Strategy to Secure Cyberspace);
- Cyber Security R&D requirements provided by customers internal to the DHS Information Analysis and Infrastructure Protection Directorate (the National Cyber Security Division and the National Communications System);
- Various cyber security research needs documents developed by the government, critical infrastructure sectors, and others;
- Discussions and coordination with members of the government research community in various interagency fora, regarding ongoing research, research needs, vulnerabilities, and threats;
- Discussions with the private sector, including both cyber security technology developer and end user perspectives.

. . . All considered in the overall context of the Department of Homeland Security Science and Technology Directorate mission.

d. You have announced the establishment this year of a Cybersecurity R&D Center.

- **Where will that center be established and what funding will it receive?)**

Answer S&T 10.d. 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. Evaluation of those proposals was completed by January 9, 2004; a technical and administrative support contract was awarded in February 2, 2004.

• How will it interact with IAIP (in particular the new cybersecurity office)?

Answer S&T 10.d The National Cyber Security Division within IAIP will provide a staff member to work with the S&T portfolio and program manager at a deputy director level.

11. Working with the Private Sector

a. Review of Vendor Solicitations: What process is the Department is using to identify useful homeland security products and technologies and reject those that are not useful or not likely to work? Once a product or technology has been identified as useful, what is the next step in the development or procurement process? How is all of this information being communicated to state and local governments?

Answer S&T 11.a. Two formal processes used to identify useful products and technologies for DHS are the formal federal funding opportunities publicly announced through the FEDBIZOPPS, and the unsolicited RDT&E proposal process.

Formal funding announcements, such as Requests For Proposals, Broad Agency Announcements, Research Announcements, etc., are used to procure goods, products, and services by DHS as well as to solicit ideas and technologies for further development. The announcements are posted on the DHS website (http://www.dhs.gov,) and the FEDBIZOPPS website (http://www.fedbizopps.gov). DHS also published a forecast of its expected fiscal year 2004 contracting opportunities over $100K on its website (See "Working with DHS"). While this forecast was prepared for small businesses, the information may be used by anyone. Usually, any business, academic group, or institution may respond to these announcements. Unless specifically justified and approved for sole source, or set aside for small business, the procurements are competitive. All responses for S&T ideas and concepts are screened by experts using a set of published criteria and those with merit are selected for funding.

The unsolicited RDT&E proposal process is run by the S&T Directorate and handles all unsolicited ideas, comments and suggestions received from the public to develop a new technology. Each unsolicited suggestion is read and assigned to one of fourteen categories for further action. These actions range from referral to another more appropriate agency, or if merited, full technical evaluation of the idea by government experts in the field. No idea or suggestion is rejected without deliberate consideration. If the unsolicited suggestion is found to be technically and programmatically sound, it then competes for funding priority with established programs. Unsolicited proposals must be scientifically valid, contain enough data to evaluate properly, and become higher priority than existing, funded programs.

If either of these methods develop a clear technology winner, DHS S&T has the capacity to carry it through prototype development to commercial production.

DHS works with state and local professional responder organizations in standards setting activities to: identify their needs, establish minimum equipment performance levels, and standardize equipment suites. Two DHS partners in this effort are the Interagency Board for Equipment Standardization and Interoperability and the Emergency Response Technology Program Advisory Board. Standards setting activities determine the criteria and test protocols that describe and evaluate required minimum levels of performance (such as for equipment, models, data, systems, and personnel) or acceptability (such as for environmental contaminants). The activities apply measurement science to develop and implement consistent, verifiable standards and test methods that measure effectiveness in terms of: basic functionality, appropriateness and adequacy for the task, interoperability, efficiency, and sustainability. Technologies and equipment that are certified by DHS have met the stipulated standards. Whether or not a product is certified, performance information will be available to state and local responders when making procurement decisions.

In addition, DHS S&T is funding the Public Safety and Security Institute for Technology (PSITEC) ($10M in fiscal year 2004) to perform the technology clearinghouse function. PSITEC develops knowledge-based services that provide access to, and distribution of, information and services relevant to public safety technologies. PSITEC will serve as the clearinghouse—a single point of entry—for the public safety and first responder community, providing access to relevant information on technologies and products, test and evaluation, as well as engaging in projects of interest and importance to them.

b. R&D Proposals by the Private Sector: In addition to the one Broad Area Announcement (BAA) that has been released regarding radiation detector

technologies, what others are planned for release in the near future? What types of R&D proposals will the Department concentrate on initially?

Answer S&T 11.b The first Broad Agency Announcement was issued on May 14, 2003 by the Technology Support Working Group (TSWG) on behalf of DHS. It closed on June 13, 2003. This BAA solicited ideas, concepts and technologies for fifty research needs in the areas of Chemical, Biological, Radiological and Nuclear Countermeasures, Explosives Detection, Improvised Device Defeat, Infrastructure Protection, Investigative Support and Forensics, Personnel Protection, and Physical Security. TSWG received 3,344 responses to this call. From these responses, TSWG requested 223 proposers to submit White Papers. Based on the evaluation of these White Papers, TSWG requested and received 47 full proposals. TSWG has completed these evaluations and is now in the contracts negotiation process. DHS has provided an initial $33M in fiscal year 2003 and an additional $30M in fiscal year 2004 to fund the most meritorious of these developments.

On 22 September, 2003, HSARPA issued its first Research Announcement (RA) for Detection Systems for Biological and Chemical Countermeasures. Its purpose is to develop, field-test, and transition to commercial production the next generation of biological and chemical detectors. This RA addresses two areas in biological countermeasures and three areas in chemical countermeasures. In response to the initial request, 518 white papers were received. One hundred twenty six proposals were received from all sources. Forty of those proposals entered negotiations for award and all are expected to complete satisfactorily.

The Homeland Security Advanced Research Projects Agency (HSARPA) issued its first Small Business Innovation Research (SBIR) Program Solicitation on November 13, 2003. The purpose of this solicitation is to invite small businesses to submit innovative research proposals that address eight high priority DHS requirements. There were 374 responses received in the eight categories and following evaluation, 66 will enter negotiations for Phase I contract award this month.

On 2 February, 2004 HSARPA published its second Broad Agency Announcement, BAA04–02, Detection Systems for Radiological and Nuclear Countermeasures. The solicitation contains six separate Technical Topic Areas. For each Technical Topic Area, respondents may submit proposals for (a.) near-term improvements incapability with rapid prototype development, (b.) development of next generation systems with significant improvements in performance, or (c.) development of enabling technologies to support next generation systems.

Additional BAAs will be issued by HSARPA in the areas of Radiological and Nuclear Architecture, Explosives Detection, Borders and Transportation Security, and Threat Vulnerability and Threat Assessment.

c. SAFETY Act: The SAFETY Act, in Section 861 of the Homeland Security Act, was established to provide contractors with the Department of Homeland Security with liability protection so they could risk placing homeland security and counter-terrorism products on the market that result in liability exposure in excess of the available insurance coverage. In order to gain the protections of the SAFETY Act, the Secretary must designate that a technology qualifies for protection pursuant to regulations to be issued by the Secretary.

• When does the Secretary intend to issue proposed and final regulations?

• Has the procurement of homeland security products been inhibited in any way by a lack of such regulations?

• Have any products been placed on the Approved Product List for Homeland Security (per section 863(d)(2) of the Homeland Security Act)?

Answer S&T 11.c. The Interim Final Rule (6 CFR Part 25) to support the Safety Act completed a second public comment period on Dec. 15, 2003. Eighteen entities made comments, with numerous comments being submitted by each entity. Comments are presently under review at DHS. A number of modifications were made to the Interim Rule after assessment of the substantive comments provided by 49 entities. The Department will address the most recent set of comments and submit the Final Rule to OMB for review in March 2004.

Applications for sellers of technologies potentially covered by the Act will be available on Sept. 1, 2003. In order to implement the Act in a rigorous, defensible, and impartial manner, extensive efforts have been underway to develop a process that will govern the evaluation of applications against the complex criteria mandated in the Act. There has also been a concerted effort to implement an electronically based application, evaluation, and tracking system that will support consistent and efficient processing of what are expected to be numerous applications. A series of 5 seminars are being held across the country in order to provide information regarding the application and evaluation process. The intent is to assist potential appli-

cants in first determining whether or not it is in their best interest to use resources to pursue SAFETY Act designation and/or certification and also to help them understand how to move through the process.

No products have yet been designated as Qualified Anti–Terrorism Technologies, nor have any yet been certified under the SAFETY Act.

12. Coordination

a. What progress has been made by the Department to date in coordinating the Department's science and technology agenda with other federal agencies to reduce duplication and identify unmet needs, consistent with the Homeland Security Act?

Answer S&T 12.a. S&T 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.

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

We are now initiating the effort needed to coordinate homeland security research and development across the entire United States Government, including the Departments of Agriculture, Commerce, Defense, Energy, Justice, Health and Human Services, State, and Veteran's Affairs; within the National Science Foundation, the Environmental Protection Agency and other Federal Agencies; and by members of the Intelligence Community.

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

We also continue to have discussions at multiple levels of management with Federal Departments and Agencies, as well as the Office of Management and Budget, the Office of Science and Technology Policy, and the Homeland Security Council to 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.

b. How does the Directorate interact with the Homeland Security Council, the President's Office of Science and Technology Policy, the National Science and Technology Council, and TSWG?

Answer S&T 12.b. Our Directorate works hard to ensure that we interact productively with the Homeland Security Council (HSC), the Office of Science and Technology Policy (OSTP), the National Science and Technology Council (NSTC) and TSWG. We are working with the Office of Management and Budget, the Office of Science and Technology Policy, and the Homeland Security Council to 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.

Our high explosives scientists are working with the Technical Support Working Group to evaluate commercial off-the-shelf systems with capabilities against suicide bombers, and the Director of the Homeland Security Advanced Research Projects Agency is a member of the TSWG Executive Committee. In addition, 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 committees and subcommittees of the National Science and Technology Council.

c. For each of the portfolios or activities you describe in your statement, please indicate what kinds of interactions and collaboration you anticipate

having with other Directorates within DHS, with other federal agencies, and with stakeholders/ providers in academia and the private sector, and how you will coordinate activities and avoid wasteful duplication?

Answer S&T 12.c The S&T Directorate has put a strong emphasis on interacting with other Federal departments and agencies and with the other components of the Department of Homeland Security. 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. Interactions are occurring between our cybersecurity personnel and those at the National Science Foundation and the National Institute of Standards and Technology, who dialog frequently and have already established collaborative and coordinated programs to ensure no duplication of effort. Our biological and chemical countermeasures staff have partnered with 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 Center for Disease Control. 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 committees and subcommittees of the 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.

In addition, the S&T Directorate has established formal liaison with the Border and Transportation Directorate, the Emergency Preparedness and Response Directorate, the Information Assurance and Infrastructure Protection Directorate, the United States Coast Guard, and the United States Secret Service. Some of these functions are fulfilled by staff from the other internal Departmental organization being matrixed to the S&T Directorate and some by S&T staff being responsible to coordinate with the other Departmental organization; in both cases, the purpose is to ensure that the S&T requirements and needs of the other components of the Department of Homeland Security are identified and addressed.

d. The Homeland Security Act transfers a number of science and technology programs from other agencies and creates several new ones—it appears that about 15 programs are created or transferred. Knitting these together into a single functioning entity is a challenge. How do you intend to accomplish that?

Answer S&T 12.d The Science and Technology Directorate has been very successful in bringing in transferred programs. Part of the reason we have been so successful in integrating pre-existing programs is the concurrent transfer of knowledgeable key personnel with the programs into our Directorate.

e. What mechanisms have been, or will be, established in the S&T Directorate to transfer homeland security technologies to federal, state, and local government, and to the private sector? If no mechanism currently exists, when does the Department intend to complete this task? Which specific office will lead it?

Answer S&T 12.e. In the Science and Technology Directorate, there are multiple mechanisms for the transfer of technologies through the private sector to state and local governments, first responders and field agents.

The Office of Systems Engineering and Development (SED) develops systems' context for solutions, conducts rapid full-scale development, conducts acceptance testing, and transitions mature technology to production and deployment. In performing its missions, SED works directly with private industry to produce affordable technology products that are of real value when purchased by the larger security community.

The Office of Planning, Programming and Budgeting has a Portfolio Manager dedicated to gathering State and Local requirements and providing information regarding the science and technology programs and developments underway. This portfolio works with State and local organizations, professional first responder associations, and other interested groups to gather and codify the science and technology requirements of the first responders.

The Homeland Security Advanced Research Projects Agency (HSARPA) directly engages the private sector. Its preferred mechanism of technology transfer is by modification or adaptation of existing products, through commercial manufacturers, to meet the immediate needs of first responders.

The Office of Research and Development will transition technologies resulting from sponsorship of research and development at the National and Federal laboratories either through SED or by allowing individual technology transfer offices at the laboratories to fulfill this function.

f. Has the S&T Directorate, or the Department overall, entered into an agreement with the Department of Energy (DoE) for the use of national laboratories? If so, please describe any such agreements that have been entered into and the specific purpose of such agreements. How does, or will, the S&T Directorate deconflict its work plan with that of DoE?

Answer S&T 12.f. In order to ensure the availability of DOE capabilities under existing site contracts, the Secretaries of Energy and Homeland Security entered into a Memorandum of Agreement (MOA), effective March 1, 2003. The objective of this MOA is to authorize a modified process for the acceptance, performance and administration of DHS work by DOE contractor and Federally operated laboratories, sites and other facilities. The MOA implements provisions of the Homeland Security Act specifying that national laboratories perform homeland security work on an equal basis with other missions at DOE sites.

13. Miscellaneous:

a. National Policy and Strategic Plan for CBRN (per sec. 302(2) of the Homeland Security Act)

• Has the national policy and strategic plan been developed? If so, please provide the Committee a copy.

• Have priorities, goals, objectives, and policies for developing CBRN countermeasures been established?

• Who is responsible for doing so?

• Do these individuals have access to the intelligence products necessary to make such judgments?

Answer S&T 13.a. National policy and strategic plan: 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 and create a national plan. The S&T Directorate takes this responsibility very seriously. We have begun this coordination process by evaluating and producing a report on the research, development, testing, and evaluation work that was being conducted within the Department of Homeland Security but was not already under the direct cognizance of the Science and Technology Directorate. Where it is appropriate, the Science and Technology Directorate will absorb these R&D functions. In other cases, the Science and Technology Directorate will provide appropriate input, guidance, and oversight of these R&D programs.

We are now initiating the effort needed to coordinate homeland security research and development across the entire United States Government. Research and development for homeland security is being conducted by the Departments of Agriculture, Commerce, Defense, Energy, Justice, Health and Human Services, State, and Veteran's Affairs; within the National Science Foundation, the Environmental Protection Agency and other Federal agencies; and by members of the Intelligence Community. Several interagency working groups already exist that are addressing issues important to homeland security. The Science and Technology Directorate has been, and continues to be, an active participant in these working groups, and in most cases has taken a leadership role. These fora foster an active exchange of information and assist each participating agency in identifying related needs and requirements, conducting research and development of mutual benefit, and avoiding duplication of effort.

We also continue to have discussions at multiple levels of management with Federal Departments and Agencies, as well as with the Office of Management and Budget, the Office of Science and Technology Policy, and the Homeland Security Council. These discussions ensure that the strongest possible links are made and

the best possible coordination occurs between our Department and those who are conducting sector-specific research. By the autumn of 2004, all Department of Homeland Security research and development programs will be consolidated and all United States Government research and development relevant to fulfilling the Department's mission will have been identified and coordinated as appropriate. It is important to note that this identification and relevant coordination does not imply the Department of Homeland Security should have the responsibility and authority for these programs within other Federal agencies; it does recognize that science and technology advances can have many applications, including homeland security.

Prioritization and Responsibility for Prioritization: The Science and Technology Directorate has prioritized its research and development (R&D) 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 Academies of Sciences 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 (R&D) needed to meet our mission requirements.

Within each portfolio, the portfolio manager (PPB) determines the final prioritization of research and development activities based on the external guidance as previously mentioned, end-user input, threat and vulnerability assessments, and subject matter expertise as provided in-house.

Intelligence inputs: S&T is currently working with the DHS Information Analysis and Infrastructure Protection Directorate to ensure that portfolio managers within S&T have the accurate and up-to-date intelligence they need to structure their portfolio's activities.

b. Nuclear Detection Technology—Is the Department aware of any technology that currently exists to detect a CBRN device within a container at our nation's ports? Is the Department actively working to develop a technology that can be used internationally and at our nation's ports to detect the presence of a CBRN device?

Answer S&T 13.b. The DHS is not aware of any existing technology that is capable of detecting all of the variety of possible chemical, biological, radiological and nuclear devices within a container. The detection of the wide variety of WMD is a challenging problem that is not solvable via a single technology which will also yield the required sensitivity and integrate into our operations.

The Department is actively working to develop technology that can be used at our nation's ports and internationally for the detection of CBRN. DHS has initiated active research and development programs targeting each of the various WMD threats; chemical, biological, and nuclear/radiological. The approach taken by S&T includes new detection technology but, more importantly, also includes development of system architectures, and the means to test different system integration concepts. Understanding system architectures, achievable detection sensitivities, and how those technologies can be integrated into existing operations is critical to understanding the effectiveness of technologies in the variety of possible architectures.

In the nuclear/radiological detection technology area, we are investigating advanced passive radiation detection technologies as well as advanced radiography and means for the direct detection of special nuclear materials. Some of these technologies are intended for the detection of radiological and nuclear threats in cargo but will be developed in a manner that most benefits security and is most easily integrated into our existing operations. These technologies will be developed such that they can, in most cases, be commercialized.

In the chemical detection technology area, toxic industrial chemical and warfare agent detectors are being developed that can be deployed to specific venues, such as ports, either permanently or as the threat requires. These technologies also can be used by the first responder for hazard identification or understanding the extent of contamination during restoration. Discussions are underway with the Bureau of Customs and Border Protection to better understand specific requirements for R&D strategic planning.

In the biodetection technology area, detect-to-warn (facility) and detect-to-treat (wide area) are being developed that can be deployed to specific venues, such as ports, either permanently or as the threat requires. These technologies also can be used by the first responder for hazard identification or understanding the extent of contamination during restoration. Currently technology for stand off detection of the biothreat is not feasible so container contents will need to be screened either through more conventional swipe and analysis. Discussions are underway with the Bureau of Customs and Border Protection to better understand specific requirements for R&D strategic planning.

c. Air Cargo Detection—Is the Department aware of technology that exists to screen air cargo before it is shipped on passenger aircraft? How mature is it? Are you aware of any efforts by the Transportation Security Administration to install such technology at our nation's airports? If not, what role, if any, is the Directorate playing in getting the technology tested and evaluated?

Existing technologies and physical inspection can be effective in screening most air cargo commodities for improvised explosive devices (IEDs). Not all technologies are good for all commodities, and physical inspection cannot be satisfactory for some shipments. However, a combination appropriately applied we believe can provide an effective air cargo screening regime. The Transportation Security Laboratory (TSL) is testing existing equipment against a broad range of commodities.

d. Cargo Mate—Please describe the S&T Directorate's current involvement in the "Cargo Mate" initiative (as referenced by Mr. Boehlert in the recent subcommittee hearing). Does the Department believe that "Cargo Mate" is a worthwhile initiative?

Answer S&T 13.d. "Cargo Mate" is a project by a commercial firm to use wireless technology to help ensure safe shipping. The S&T Directorate has no current or prior involvement in the "Cargo Mate" Initiative identified in the question and has no basis to evaluate the initiative.

14. Question from Rep. Kendrick Meek, Subcommittee Member—Please comment on how the Department plans to use and fund social and behavioral science research that goes to the heart of the Homeland Security mission, such as: psychological and sociological research on how terrorists act and think, statistical data analysis as relates to law enforcement and the nation's transportation infrastructure, and international relations research on how U.S. foreign policy impacts the campaign against terrorism worldwide.

Answer S&T 14. S&T's social and behavioral sciences terrorism studies program goes to the heart of the U.S. Homeland Security mission by focusing on the current and future (dynamic and escalating) terrorism threat environment and employing a comprehensive and multidisciplinary social and behavioral sciences approach. Leading edge conceptual methodologies and tool kits will be employed to help the homeland security—and wider combating terrorism—communities better understand how to assess, model, forecast and preemptively respond to current and future terrorist threats, whether conventional low impact, conventional high impact, or CBRN—with the latter two types of warfare considered high impact catastrophic attacks.

Two primary research and analysis projects will be conducted during fiscal year 2004 and fiscal year 2005, with the third project the creation of a comprehensive open-source-based Global Terrorist Incident Database (linked to other on-going databases), with a robust social sciences methodological computerized engine, to be used to generate a spectrum of indicators, including measuring and mapping combating terrorism effectiveness, that will be used to support the program's projects. Above all, the findings from all the projects will be widely disseminated throughout the Homeland Security (and combating terrorism) community via a Web Portal that will serve as a knowledge-base and interactive 'virtual community.'

The first project comprehensively addresses the primary components in how terrorists act and think by focusing on the terrorist life cycle (TLC) and terrorist attack cycle (TAC). It begins with the study of the underlying root causes of terrorism

which give rise to terrorist insurgencies. To bring scientific rigor to such a study, a root cause analysis software tool kit, developed for the business world, will be adapted to hierarchically decompose and map all the significant root causes listed in the academic and practitioner literature on terrorism. Such a methodological approach has never before been applied to the study of terrorism, so this is one example of how our approach will advance the state of the terrorism analytic discipline. A second example of the uniqueness of our approach is the use of a link analysis tool kit to diagram the formal and informal organizational structures and linkages among terrorist groups, including various front organizations (political, commercial or charity), in groups such as al Qaida and its affiliates, which pose the greatest threat to the U.S. Homeland and overseas interests. Both of these sets of diagrams will be used to structure follow-on research, including the first research effort, followed by an experts' workshop, that will use such data to identify, vet and prioritize key nodes and linkages in the TLC and TAC that may be most vulnerable to counteraction and influence. This will include (but not limited to) such indicators as the nature of a group's leadership, its ideology and strategy, its modus operandi, including recruitment patterns, developing a support infrastructure, attaining the capability to launch a spectrum of attacks, and choosing targets and their locations. In a second research effort, followed by an experts' workshop, the project will then seek to identify, vet and prioritize those counterterrorist measures that could be used to influence those nodes and linkages in the TLC and TAC deemed most vulnerable or most crucial to counteract. The third research effort will attempt to formulate metrics for assessing counterterrorism effectiveness, which will be discussed, vetted and prioritized by the third experts' workshop. A comprehensive report on findings, including templates of the root causes and organizational formations diagrams, will then be disseminated to the homeland security's (and wider combating terrorism's) scientific and operational communities.

The second project will utilize the multi-disciplines of the social, behavioral and cognitive/neurosciences, combined with subject matter and operational expertise of military, law enforcement, and intelligence professionals, to better understand and respond to suicide terrorism, at the individual, group, and societal levels. Academic, scientific and operational experts will form the study team for the project. Following initial research, a series of expert workshops will be held. The National Institute of Mental Health (NIMH) is interested in co-funding the project. A monograph will be produced and disseminated to the homeland security's (and wider combating terrorism's) scientific and operational communities.

Adopting such a multi-disciplinary approach is expected to greatly advance the state of the discipline on this problem area. The challenge of counteracting suicide attacks as an asymmetric instrument of terrorism is one of increasing concern and severity, not only in the Middle East but elsewhere around the globe. While significant social and behavioral research on this phenomenon has been ongoing, it is still in a relatively early stage and has yet to fully involve some of the social science disciplines that could enhance understanding of the problem and potential programmatic approaches to its counteraction.

The objective of the research program is to study the underpinnings, processes, life cycles and attack cycles of those who manage and engage in suicide terrorism within the framework of the groups, societies and religions that encourage and perpetuate such activities. The results of this program, including study efforts and workshops of area experts will be important in the formulation of effective and forward-learning behavioral and technological responses. The proposed program will be conducted over the course of two fiscal years (fiscal year 2004 and fiscal year 2005), with interim results being provided as they become available.

In addition to these two primary research projects, and creation of the Web Portal, the social and behavioral program is contributing to the Homeland Security mission in several other important areas.

- First, the program's manager serves as the co-chair of an interagency working group, under the White House Office of Science & Technology Policy, on how the social, behavioral and economic sciences can be used to support counterterrorism, by prioritizing research areas for government agencies.
- Second, the program will be leveraging the expertise acquired in its projects to contribute to the social and behavioral communities on these issues, such as the national laboratories, the National Science Foundation, the National Academy of Science, and the scientific and academic communities, as well as the homeland security's (and combating terrorism's) operational communities.

15. Question from Rep. Jane Harman, Member of the Full Committee—The Department of Homeland Security will need to integrate data from disparate source systems in order to provide analysts and enforcement agen-

cies with timely information for further action. Has the Science and Technology Directorate researched and evaluated commercially-available data fusion and analytic technologies that are capable of providing predictive analysis (including of non-obvious relationships) and able to meet anticipated volumes of data and speed of response? If so, can you provide a summary of your findings and recommendations? If this research has not yet been done, is it part of your areas for effort in fiscal year 2004?

Answer S&T 15. Information analysis and data fusion are encompassed within the technologies being investigated through the Threat and Vulnerability, Testing and Assessment (TVTA) Portfolio in S&T. The portfolio is also investigating two closely related technology areas, namely, collaboration tools and advanced visualization techniques, as part of its effort to provide analysts with a near-real time capability to find, retrieve, integrate, and analyze information from multiple, distributed, disparate data sources. These technologies will form the basis for the so-called Threat-Vulnerability Integration System (or TVIS), for which TVTA initiated in fiscal year 2004 a research and development program as well as a prototyping effort. The efforts are being addressed through both intramural research with the National Laboratories and a comprehensive research effort with commercial vendors through a BAA. For fiscal year 2004, the approach is to seek advanced technologies that address the specific, immediate requirements of the Department's Information Analysis and Infrastructure Protection Directorate rather than initiate a test and evaluation program for commercial tools. Creating a testbed enabling ongoing, comprehensive evaluation of advanced analysis, visualization, and collaboration tools—from the commercial, private, and government sectors—is planned for fiscal year 2005.

APPENDIX

APPENDIX A—PEER REVIEW PROCEDURES (OFFICE OF RESEARCH AND DEVELOPMENT)

REVIEW AND SELECTION OF PROPOSALS FROM THE U.S. DEPARTMENT OF ENERGY NATIONAL LABORATORIES TO THE U.S. DEPARTMENT OF HOMELAND SECURITY SCIENCE AND TECHNOLOGY DIRECTORATE RADIOLOGICAL AND NUCLEAR COUNTERMEASURES PORTFOLIO

MICHAEL J. BURNS

OFFICE OF NATIONAL LABORATORIES

OFFICE OF RESEARCH AND DEVELOPMENT

SCIENCE AND TECHNOLOGY DIRECTORATE

U.S. DEPARTMENT OF HOMELAND SECURITY

AUGUST 14, 2003

Abstract

The process to be followed by the Office of National Laboratories (ONL) to make recommendations for the placement of work at DOE National Laboratories from the Rad/Nuc Countermeasures portfolio is detailed here. Submissions responsive to needs expressed by the Rad/Nuc portfolio manager are expected from two consortia of national laboratories by August 25, 2003. These submissions will be organized into sections containing detailed project proposals. Each proposal will be subjected to both a semi-quantitative numerically-scored review consisting of Technical Merit, User Relevance, and Execution Planning components, as well as an overall Management Assessment. The Technical Merit portion of the review will be conducted by external reviewers utilizing the ORISE PeerNet system and organized with separate review teams for each section of the submissions. Numerical scores for all three scored components will be assigned based upon criteria listed in this paper and an overall numerical score calculated with a weighting of 40% assigned to the first two components and 20% assigned to the third. The scored portion of the review will be combined with the outcome of an overall Management Assessment that consider inputs and issues not well-captured by the scored portion of the review. The scored rankings and the Management Assessment will form the basis for ONL's recommendations for work assignment to the labs. ONL will present these recommendations to the Director, Office of Research and Development (ORD) for funding decisions. The remaining fiscal year 03 funds will be distributed and fiscal year

04 plans made (with fiscal year 04 funding awaiting congressional action to establish the DHS fiscal year 04 budget) based upon ORD's decisions. ORD decisions will be certified by the Director, Office of Plans, Programs, and Budgets (PPB). ONL anticipates the funding decisions to be made by September 19, 2003.

I. Introduction

The U.S. Department of Homeland Security's (DHS) Science and Technology Directorate (S&T) has solicited proposals from certain U.S. Department of Energy (DOE) National Laboratories to execute new programs within the Directorate's Radiological & Nuclear (Rad/Nuc) Countermeasures Portfolio. Although this portfolio has many on-going programs that are underway at some national laboratories, a significant amount of new work is scheduled to begin and is intended for execution at DOE's national labs. Assignment of this work will be made through the review of specific laboratory proposals made in response to S&T's Rad/Nuc portfolio needs. It is the purpose of this paper to outline the process that S&T's Office of National Laboratories (ONL) will use to review proposals and make recommendations to the Director, Office of Research and Development (ORD) for the ultimate placement of work at the labs.

Section II of this paper presents a brief overview of the Rad/Nuc portfolio that is intended as useful background for those considering the review process. Section III of this paper presents the general structure expected of the laboratory submissions and also discusses the subsequent review process. This section outlines some specific requirements of the labs in formatting and delivering their submissions. It also presents an overview of the review process. Section IV summarizes the PeerNet system hosted by the Oak Ridge Institute for Science and Education (ORISE) that will be used by external reviewers to enter their comments regarding specific proposals. PeerNet is an established system for independent anonymous review of technical proposals and provides a convenient method to capture reviewer comments, organize them efficiently for DHS S&T review, and to maintain documentation of the review process. PeerNet has been used extensively by certain U.S. Government agencies for this purpose in the past. Section V presents the review criteria that will be used by the various reviewers who will examine the laboratory proposals. Criteria are listed here for both the numerically-scored components of the review and the Management Assessment. Finally, Section VI provides a discussion of the dates associated with this review and a check-list of actions required by the laboratories in support of the review.

II. Overview of the Radiological and Nuclear Countermeasures Portfolio

The technology, materials, and expertise required to build radiological and nuclear weapons are spreading inexorably. The Department of Homeland Security's Science and Technology Directorate has developed the Radiological and Nuclear Countermeasures Portfolio to develop science and technology useful in addressing this pressing homeland security issue. The portfolio strategy is comprehensive: securing existing materials; providing technologies for detection of radiological materials at the nation's borders and in transit within the transportation infrastructure; and providing an effective intervention capability at the local, state, and federal level. The portfolio will also support the development of the best available technologies, training, and information to assist in crisis response, incident management and recovery, and attribution.

The Rad/Nuc portfolio focuses on providing federal, state, and local end users (including Borders and Transportation Security agencies, Emergency Preparedness and Response agencies, the U.S. Coast Guard, and port authorities) 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 the nation's borders. Key initiatives include the deployment, evaluation, and evolution of currently available technologies at ports of entry; the development and prototyping of systems for detection within the transportation infrastructure; the development of advanced technologies for more effective crisis response at the time of an event; and the development of an effective, science-based consequence management program. The portfolio will also provide an enduring science and technology base for addressing such long-term challenges in radiological and nuclear detection systems as the detection of Highly–Enriched Uranium (HEU) and shielded plutonium and radioactive sources. Technical expertise will also be provided to the operational directorates of DHS as needed and the performance of deployed systems will be continually assessed to identify vulnerabilities and opportunities for improvement.

Assessment of proposals submitted in support of Rad/Nuc portfolio goals will require a broad cross-section expertise that could include nuclear science, nuclear

chemistry, engineering, nuclear medicine, systems analysis, and emergency response.

III. General Structure of Submissions and Review

ONL expects two large submissions from two groups of DOE national laboratories. These submissions will contain specific proposals to execute work in response to needs outlined by the S&T Rad/Nuc portfolio manager in a briefing to the laboratories given on July 22, 2003 in Washington, DC. Each of the two submissions will contain major sections as described during the ONL/National Laboratories meetings on this subject conducted July 22–23, 2003 in Washington, DC. Each section will contain specific proposals for work in support of the Rad/Nuc portfolio. These specific proposals must be contained in separate files.

ONL has been notified that the Lawrence Livermore National Laboratory (LLNL), the Los Alamos National Laboratory (LANL), and the Sandia National Laboratory (SNL) will be the principal authors of one submission. This submission may also contain work that is proposed for execution at other national laboratories. ONL has also been notified by the Argonne National Laboratory (ANL), Bechtel/Nevada (BN), the Brookhaven National Laboratory (BNL), the Idaho National Environmental and Engineering Laboratory (INEEL), the Oak Ridge National Laboratory (ORNL), and the Pacific Northwest National Laboratory (PNNL) that this group of laboratories will team as principal authors to generate a second submission. Again, this submission may have roles identified for other institutions.

Each submission must be delivered electronically in files formatted in standard ".pdf" format. Electronic submission will be made to the PeerNet website according to instructions that will be supplied to the labs in the near future. Authors can check the web-site at www.orau.gov/dhsuce for a similar site. Questions concerning submission should be directed to the Deputy Office Director of ONL (Dr. Caroline Purdy, Caroline.Purdy@dhs.gov).

Each submission must be received by 8:00 a.m., EDT, on August 25, 2003.

Each submission must be clearly separated into distinct sections that roughly align with the Work Breakdown Structure devised for the Rad/Nuc portfolio. These sections will be used by ONL to organize proposals for separate review groups. The major elements of the Rad/Nuc portfolio Work Breakdown Structure are Systems Architecture and Pilot Deployments, Pre–Planned Product Improvement, Technology Development Initiatives, and Incident Management. In the July 22–23, 2003 ONL/National Laboratories meeting concerning the Rad/Nuc portfolio, it was agreed that there was not significant National Laboratory work in the Pre–Planned Product Improvement WBS element. The Laboratories also indicated a preference for organizing their proposals into sections that represented broad capabilities. Finally, ONL desired to group the proposals into major categories for which separate review teams could be formed. Therefore, there should be six major sections for each submission. These sections are :

1. Systems Analysis and Integration
2. Pilot Demos
3. Passive Detection Technology
4. Active Detection Technology
5. Pre–Event Incident Prevention and Response
6. Post–Event Incident Prevention and Response

The Systems Analysis and Integration section is to contain proposals addressing systems analysis, systems integration, and sensor network needs shown in the Rad/Nuc portfolio briefing on July 22, 2003. The Pilot Demos section is not to include the ongoing New York/New Jersey Port Authority project but should include proposals addressing surreptitious entry needs from the Rad/Nuc portfolio briefing and any additional work concerning TSA or other operational elements, representative pilot demos, etc. The Passive and Active Detection Technology sections are self-explanatory and the detailed needs listed in the July 22 briefing should be addressed. The Pre-Event Incident Prevention and Response section should include all attribution material.

Each submission must be clearly separated into these areas so that ONL and ORISE can present each to a separate review team. Each section should contain specific, individual proposals for work. Each of the individual proposals should be contained in a separate ".pdf" file. Each proposal should each have a specific, unique name, and be associated with a specific section of the submission. The PeerNet system will also generate a unique numerical designation for each proposal. Each proposal should be responsive to the goals and objectives of the Rad/Nuc portfolio or include work that falls within that DHS mission space. Each proposal must represent a clearly defined project or research effort, with clearly defined objectives or problems to be addressed, clearly defined assumptions, clearly defined methods of

accomplishment (including as much detail as possible on facilities, techniques, and personnel to be used), clearly defined deliverables, a clearly defined schedule, and a clearly defined cost.

S&T will choose to fund laboratories at the proposal level and will not necessarily be choosing one of the two consortia submissions over another. Instead, S&T will consider each proposal in each section of the submissions. The final assignments made by S&T are expected to consist of a mixture of proposals from each submission.

Each proposal will be subjected to two types of review. The first will be a semi-quantitative, scored review. The second type will be a management assessment that considers issues and inputs difficult to address using the scored system.

The scored review has three components. These components are Technical Merit, User Relevance, and Execution Planning. Numerical scores will be given for each of several criteria that are defined below for each component. An overall numerical score will be generated by weighting the scores for each component. Technical Merit will account for 40% of the overall score. User Relevance will also account for 40% of the final score. Execution Planning will account for the remaining 20%.

Independent technical experts shall be utilized by ONL to conduct the Technical Merit component of the scored review. These experts will be selected from organizations such as the American Physical Society, the American Chemical Society, academia, other government agencies, or private industry. National Laboratories will not be asked to provide reviewers. The reviewers will be grouped into teams of 3–4 persons with each team reviewing a separate section of the submissions. Numerical scores will be given according to the Technical Merit criteria discussed below and entered by the reviewers into the PeerNet system. Telephone conferences will be held between ONL and the reviewers before the review begins and near the end of the review. During the second conference, ONL will check to see if there are unanswered questions that could affect the final scoring of proposals. If such questions exist that can be answered quickly, ONL or the reviewers will contact the proposal authors for clarification and the results of that contact considered before the Technical Merit component of the review is finalized.

The User Relevance component of the scored review will permit user input to influence the selection of proposals to be funded. ONL will ask S&T portfolio managers that represent DHS operational elements to serve as reviewers for this component of the review. Portfolio managers representing the U.S. Coast Guard, U.S. Secret Service, the DHS Borders and Transportation Security Directorate, the DHS Information Analysis and Infrastructure Protection Directorate, and the DHS Emergency Preparedness and Response Directorate will serve as reviewers to score each proposal that could impact their area of responsibility according to the User Relevance criteria below.

Finally, the Execution Planning component of the scored review will be conducted by the Portfolio Manager and Program Managers of the Rad/Nuc portfolio and the ONL Director and Deputy Director. The criteria for this component are also shown below.

Upon conclusion of the scored review, a Management Assessment review will be conducted. This review is necessary to consider inputs and issues that are not well captured by the scored part of the review. These inputs and issues are listed in the Review Criteria section below as well. The Management Assessment will be conducted by the ONL Director with assistance from the ONL Deputy Director and the Portfolio Manager and Program Managers of the Rad/Nuc portfolio

Upon completion of the scored components of the review and the Management Assessment, ONL will compile a rank-ordered list of proposals for each of the three major sections of the national laboratory submissions. These rank-ordered lists of proposals and ONL's recommendations for funding actions will be presented to S&T's Director, Office of Planning, Programs, and Budgets (PPB), and Director, Office of Research and Development (ORD). The final decision as to which proposals will be funded will be made by the ORD Director, a federal government employee. The PPB Director will certify this decision and be S&T's final signature on funding documents that will move funding and authorization to the laboratories.

Finally, ONL will furnish documentation of the review including a proposal evaluation form that will summarize the results of the review for each proposal in each section of the submissions.

IV. PeerNet

PeerNet is a secure, web-based peer review system maintained by the Oak Ridge Associated Universities (ORAU) through its operation of the Oak Ridge Institute for Science and Education (ORISE) for the U.S. Department of Energy. Neither ORAU nor ORISE are associated with ORNL. Annually, ORAU coordinates over 30 panel and postal reviews involving more than 1,300 reviewers of over 1,600 proposals for DOE, the Pennsylvania Department of Health, and now DHS. ORAU coordinated 96% of the peer reviews for the DOE Office of Science in fiscal year 2002.

PeerNet was used to record reviewer scores and comments and provide reports to the sponsors of the review. The scientific focus areas of the fiscal year 2002 reviews were varied and included biomedical, clinical, and health services, as well as science, energy, defense, and environmental programs. This system was designed to streamline collecting, tabulating, and reporting evaluative comments and/or scores from multiple reviewers with common criteria. It has a straightforward interface to provide access to significant flexibility for each peer review.

ORAU also has access to extensive professional networks to recruit and select reviewers with the necessary expertise for each review, including an 86-member university consortium and councils, other universities, relevant professional organizations, and public lists. We will access ORAU's list of possible reviewers and combine it with S&T's contacts to establish credible review panels for each section of the laboratory submission.

After selection by ONL, each reviewer will sign a conflict of interest form to ensure that each reviewer is an uninterested external examiner of the proposal. They will then be assigned by ORISE a password for access to the secure portion of PeerNet. Electronic versions of each laboratories submission will be posted on PeerNet. ORISE or ONL will have separated each submission into its component sections and will have organized each section into its component proposals. Each proposal will be associated with one of the two submissions and carry a unique title provided by the submission authors. A unique numerical identification number will also be associated with each proposal by the PeerNet operators. To support this system, it is therefore necessary for each submission to be provided to ONL electronically in standard ".pdf" format.

Each reviewer will read the proposals on-line and score them according to the criteria below. Each reviewer will also enter their individual comments as needed. Any questions, especially those that affect the reviewers final scoring, will be noted by ONL. The submission authors will be provided an opportunity to respond to question with a rapid one- or two-day turnaround. Therefore, authors will not be able to rewrite the proposal, but will be able to offer clarifications.

Upon receipt of any answers that were requested, reviewers will conclude their review. ORISE will then compile the results as directed by ONL.

We anticipate that PeerNet will be used for all components of the scored portion of the review.

V. Review Criteria

The scored components of the review will use a scoring system running from 1 to 4. Generally, a value of 1 is assigned to excellent proposals and 4 to poor proposals. The Technical Merit and User Relevance components of the scored review will also include a single qualitative indicator as shown below.

To the extent possible consistent with delivery of submissions by August 25, authors are encouraged to write their proposals as clearly as possible with respect to the review criteria shown below. In this way, reviewers will be more likely to consider all information that the laboratories think is important for each reviewer to complete the evaluation.

The Technical Merit component of the review will apply a numerical score for "technical merit" and a second numerical score for "technical team" as shown below. A single qualitative indicator for "technical risk assessment" will also be provided. The Technical Merit scoring criteria are:

"Technical Merit"

1. Scientifically and technically sound; technical approach is clear and appropriate
2. Scientifically and technically sound, but there are minor questions about the technical approach or underlying assumptions
3. There are one or more significant questions about the technical approach or the scientific/technical basis of this proposal
4. Scientifically or technically unsound; OR the technical approach is very unclear, missing, or inappropriate

"Technical Team"

1. The Principal Investigator (PI, if identified) and team have an established record of technical achievement in this area or in closely related work
2. The PI and team have an established record in an area that is indirectly related to the proposed work
3. The PI and team are generally experienced in related work, but have little or no track record in the area of the proposal
4. The PI and team's record is poor

"Technical Risk Assessment"

"Low"—straightforward technical path, no significant challenges or impediments to success
"Medium"—moderately difficult technical path; impediments can probably be overcome
"High"—very challenging technical path; impediments could prevent successful outcome

The User Relevance component of the review will apply a numerical score for "alignment with DHS missions and needs", a second numerical score for "time to return-on-investment", and a third numerical score for "difficulty of user implementation (assuming technical success)", as shown below. A single qualitative indicator for "operational risk assessment" will also be provided. The User Relevance scoring criteria are:

"Alignment with DHS missions and needs"

1. The outcome of the proposed work is highly aligned with the broad missions and needs of DHS; meets a goal in the Rad/Nuc PADs; a specific DHS user community is highly interested in the outcome of the proposed work.
2. The outcome of the proposed work is generally aligned with the broad missions and needs of DHS, although it is not in the Rad/Nuc PADs; there is general interest from one or more DHS user communities
3. The outcome of the proposed work is clearly not aligned with the broad missions and needs of DHS and is not in the Rad/Nuc PADs; no DHS user community has expressed interest, but interest should be solicited before proposal disposition is decided
4. The outcome of the proposed work is not relevant to the missions and needs of DHS; OR no DHS user community has expressed an interest and solicitation of interest is not recommended

"Time to return-on-investment"

1. The outcome of this work is likely to impact a relevant DHS user group in less than 2 years
2. The outcome of this work is likely to impact a relevant DHS user group in 2–5 years
3. The outcome of this work is likely to impact a relevant DHS user group in 5–10 years
4. The outcome of this work may impact a relevant DHS user group in 5–10 years, but DHS funding is not appropriate

"Difficulty of user implementation (assuming technical success)"

1. Straightforward implementation; no significant challenges to implementation
2. Moderately difficult; implementation challenges can probably be overcome
3. Very challenging; there are significant difficulties to implementation, but implementation is plausible
4. Too challenging; there are significant difficulties to implementation so that implementation is not plausible

"Operational Risk Assessment"

"Low"—straightforward; no significant challenges or impediments to success
"Medium"—moderately difficult; impediments can probably be overcome
"High"—very challenging; impediments could prevent successful outcome

The Execution Planning component of the review will apply a numerical score for "project management plan", a second numerical score for "Resources (people and facilities)", and a third numerical score for "overall plan execution risk", as shown below. The Execution Planning scoring criteria are :

"Project management plan"

1. Plan is very clear and credible; tasks, milestones, and deliverables are well defined; proposed funding is consistent with the scope of the project
2. Plan is generally clear and credible, but there are minor questions about tasks, milestones, deliverables, or funding levels
3. There are one or more significant questions about the project management plan (tasks, milestones, deliverables, or funding levels)

4. Plan is missing, unclear, or not credible; OR significant prior deliverables for the project have not been met

"Resources (people and facilities)"

1. The proposed technical team, facilities, and resources are known to be available at the necessary level and the resource plan includes all required resources
2. The proposed technical team, facilities, and resources are not complete or not fully available, but the gap can probably be filled without significant difficulty
3. The reviewer has one or more significant questions concerning the proposed technical team, facilities, and resources, and it is not clear that these gaps can be filled without significant difficulty
4. The proposed technical team, facilities, and resources have significant gaps or questions that are not likely to be addressed.

"Overall Plan Execution Risk"

1. Risk for successful execution is acceptable or a robust mitigation plan is in place
2. A risk mitigation plan has been prepared and is plausible
3. There are multiple risks with questionable mitigation strategy
4. Risk is considered too high; risk mitigation plan is unacceptable or not identified

After the scored components of the review have been compiled, an overall Management Assessment of the proposals will be conducted to address inputs and issues not captured by the scored components of the review. The final ranking of the proposals will consider both the scored results and the qualitative results of the Management Assessment. The list of issues that will be considered during the Management Assessment include :

A. The possibility of congressional language or guidance
B. S&T strategy for the development of a manageable intramural national laboratory capability
C. The total funding available to the portfolio
D. The balance of risk for all projects across the portfolio (S&T believes that risk is not inherently bad, but we seek the right balance of low, medium, and high risk projects)
E. The merit of proposals or approaches that show innovation to address problems in a way S&T of the DHS User Community had not considered
F. Integration with other S&T portfolios, other DHS directorates, and other federal agencies, such as DOE/NNSA.
G. The overall technical and program execution performance of the proposed technical team for similar projects in the past.

VI. Dates and Check List.

July 22 ONL/National Laboratories meeting to present details from the Rad/Nuc portfolio and develop structure for proposal submissions

Aug. 25 Laboratory submissions received at ONL by 8:00am EDT. ONL and ORISE parse the submissions and install in PeerNet. ONL distributes to other reviewers as needed, including User Relevance reviewers and Management Assessment reviewers.

Sept. 5 Initial technical merit review closes

Sept. 8 ONL compiles initial technical merit review results and distributes to the National Laboratories any clarification questions that may have been developed.

Sept. 9 First session of User Relevance review.

Sept. 10 National laboratories provide responses as needed to requests for clarification from technical merit review. ONL distributes responses to technical reviewers as needed. Technical reviewers use these responses to finalize their review.

ONL distributes to National Laboratories any requests for clarification that May have been developed in the first session of the User Relevance Review.

Sept. 12 Technical Merit review is finalized.

National Laboratories respond by the beginning of the day with responses that may be required to complete the User Relevance review.

Second and final session of the User Relevance review.

Sept. 15 ONL compiles final results of the Technical Merit and User Relevance reviews.

Sept. 16 Management Assessment review and development of ONL recommendations

Sept. 17–18 ONL delivers recommendations to ORD and PPB

Sept. 19 Funding decisions by ORD, certified by PPB, provided to ONL. Processes to distribute funds initiated.

The following checklist for National Laboratory submissions may benefit the principal authors to ensure the submissions can be effectively evaluated by S&T.

Organize the overall submission with six clearly identified sections as shown below:

1. Systems Analysis and Integration
2. Pilot Demos
3. Passive Detection Technology
4. Active Detection Technology
5. Pre–Event Incident Prevention and Response
6. Post–Event Incident Prevention and Response

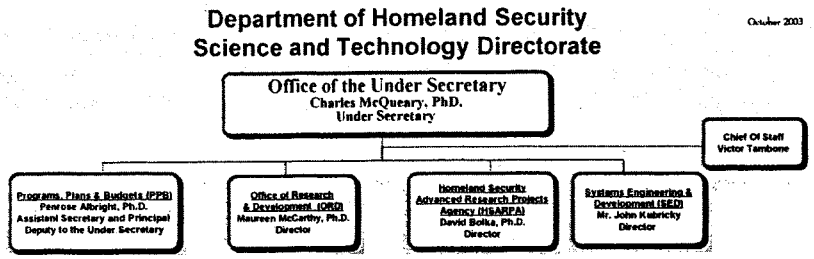
Ensure each section contains clearly identified proposals. Each proposal is contained in a separate ".pdf" file. Each proposal must represent a clearly defined project or research effort, with clearly defined objectives or problems to be addressed, clearly defined assumptions, clearly defined methods of accomplishment (including as much detail as possible on facilities, techniques, and personnel to be used), clearly defined deliverables, a clearly defined schedule, and a clearly defined cost.

Submissions must be received by 8:00am, EDT, August 25, 2003. Submissions must be in the standard ".pdf" format.

Be prepared to respond to possible requests for clarification from ONL concerning the Technical Merit review on Sept. 8, 2003 with responses due on Sept. 10, 2003.

Be prepared to respond to possible requests for clarification from ONL concerning the User Relevance review on Sept. 10, 2003 with responses due at the start of business, eastern time, on Sept. 12, 2003.

Appendix B – Science and Technology Directorate Organizational Chart



Appendix C is being retained in the Committee's files.

Appendix D—NIST/DHS MOU

MEMORANDUM OF UNDERSTANDING

between the

DIRECTORATE OF SCIENCE AND TECHNOLOGY,

U.S. DEPARTMENT OF HOMELAND SECURITY

and the

TECHNOLOGY ADMINISTRATION,

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY,

U.S. DEPARTMENT OF COMMERCE

I. PURPOSE

The Department of Homeland Security ("DHS") Science and Technology Directorate ("Directorate") is developing technological tools to protect our nation's homeland. Successful development, testing, evaluation, and deployment of these technologies require expertise in measurement science and in the development of standards. The Directorate intends to take advantage of the significant capabilities that exists in these areas within the Department of Commerce's Technology Administration ("TA"), specifically at the National Institute of Standards and Technology ("NIST"). Therefore, wherever possible and mutually beneficial, the Directorate and TA seek to collaborate on research and planning activities, and share where appropriate facilities, personnel, and scientific information. This Memorandum of Understanding (MOU) sets forth the basic principles and guidelines under which the parties will work together to accomplish these goals.

II. Authority

Authority for cooperation in areas of overlapping interests and responsibilities is provided for the Directorate pursuant to the authority of Public Law 107–296, The Homeland Security Act of 2002 that established DHS and for NIST, under the National Institute of Standards and Technology Act (15 U.S.C. 271 et. seq.)

III. Implementation

(a) In order to enable close and effective collaboration, it is agreed that the scope of cooperative activity will be reviewed annually. Both the Directorate and TA will identify managers to implement and coordinate the MOU. The managers shall meet on a regular basis to discuss and direct activities conducted under the MOU.

(b) The managers shall obtain appropriate express written agreement by the Directorate and TA on each significant activity to be undertaken pursuant to the MOU—including consensus on the scope of work; deliverables (if any) and delivery dates; anticipated products and outcomes; periods of performance; levels of funding and resources to be provided for each activity by the parties; and any other appropriate and necessary aspects of mutual activities.

(c) Costs associated with the participation of the Directorate and TA shall be subject to the availability of appropriated funds and designated personnel of each party, or the approval of other sources of funding. Funding for, and resources allocation to, each significant activity undertaken pursuant to this MOU shall be arranged in accord with the applicable written implementing agreement of the parties required in the above paragraph II(b).

(d) Costs associated with participation by Directorate-supported personnel who use TA facilities and resources, including equipment, laboratory, and office facilities, will be provided through the Directorate. Costs associated with participation by TA-supported personnel who use the Directorate's facilities and resources, including equipment, laboratory, and office facilities, will be provided through TA.

(e) The managers shall seek to resolve any dispute concerning the MOU through good-faith discussions.

IV. EFFECTIVE DATE

This MOU is effective upon signature of the parties and will remain in effect unless and until terminated as provided under Article VI.

V. AMENDMENTS

This MOU may be modified or amended by written agreement among the parties hereto. Additionally, any terms or conditions involving the Directorate and TA not stated in this MOU but expressly agreed to in a future MOU signed by the Secretary of the Department of Homeland Security and the Secretary of the Department of Commerce is considered integrated into this MOU.

VI. TERMINATION

This MOU will expire sixty (60) months from the date of execution unless renewed by mutual agreement of the parties. This MOU may be terminated at any time by mutual agreement of both parties. Expiration or termination would affect only pursuit of new projects under the MOU. Projects under way will be governed by the specific individual agreements anticipated above.

AGREED TO BY:

Charles E. McQueary
Under Secretary for Science and Technology
Technology Administration
U.S. Department of Homeland Security
On this date: May 22, 2003

Phillip J. Bond
Under Secretary for Technology
Science and Technology Directorate
U.S. Department of Commerce
On this date: May 22, 2003

○