THE DEPARTMENT OF HOMELAND SECURITY'S R&D BUDGET PRIORITIES FOR FISCAL YEAR 2008

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION

COMMITTEE ON SCIENCE AND TECHNOLOGY

HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

MARCH 8, 2007

Serial No. 110–8

Printed for the use of the Committee on Science and Technology

Available via the World Wide Web: http://www.house.gov/science

U.S. GOVERNMENT PRINTING OFFICE
33–611PS WASHINGTON : 2007

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

COMMITTEE ON SCIENCE AND TECHNOLOGY

HON. BART GORDON, Tennessee, *Chairman*

JERRY F. COSTELLO, Illinois
EDDIE BERNICE JOHNSON, Texas
LYNN C. WOOLSEY, California
MARK UDALL, Colorado
DAVID WU, Oregon
BRIAN BAIRD, Washington
BRAD MILLER, North Carolina
DANIEL LIPINSKI, Illinois
NICK LAMPSON, Texas
GABRIELLE GIFFORDS, Arizona
JERRY MCNERNEY, California
PAUL KANJORSKI, Pennsylvania
DARLENE HOOLEY, Oregon
STEVEN R. ROTHMAN, New Jersey
MICHAEL M. HONDA, California
JIM MATHESON, Utah
MIKE ROSS, Arkansas
BEN CHANDLER, Kentucky
RUSS CARNAHAN, Missouri
CHARLIE MELANCON, Louisiana
BARON P. HILL, Indiana
HARRY E. MITCHELL, Arizona
CHARLES A. WILSON, Ohio

RALPH M. HALL, Texas
F. JAMES SENSENBRENNER JR., Wisconsin
LAMAR S. SMITH, Texas
DANA ROHRABACHER, California
KEN CALVERT, California
ROSCOE G. BARTLETT, Maryland
VERNON J. EHLERS, Michigan
FRANK D. LUCAS, Oklahoma
JUDY BIGGERT, Illinois
W. TODD AKIN, Missouri
JO BONNER, Alabama
TOM FEENEY, Florida
RANDY NEUGEBAUER, Texas
BOB INGLIS, South Carolina
MICHAEL T. MCCAUL, Texas
MARIO DIAZ-BALART, Florida
PHIL GINGREY, Georgia
BRIAN P. BILBRAY, California
ADRIAN SMITH, Nebraska
VACANCY

SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION

HON. DAVID WU, Oregon, *Chairman*

JIM MATHESON, Utah
HARRY E. MITCHELL, Arizona
CHARLIE A. WILSON, Ohio
BEN CHANDLER, Kentucky
MIKE ROSS, Arizona
MICHAEL M. HONDA, California
BART GORDON, Tennessee

PHIL GINGREY, Georgia
VERNON J. EHLERS, Michigan
JUDY BIGGERT, Illinois
JO BONNER, Alabama
ADRIAN SMITH, Nebraska

RALPH M. HALL, Texas

MIKE QUEAR *Subcommittee Staff Director*
RACHEL JAGODA BRUNETTE *Democratic Professional Staff Member*
COLIN MCCORMICK *Democratic Professional Staff Member*
SHEP RYEN *Republican Professional Staff Member*
AMY CARROLL *Republican Professional Staff Member*
MEGHAN HOUSEWRIGHT *Research Assistant*

CONTENTS

March 8, 2007

Page

Appendix: Answers to Post-Hearing Questions

THE DEPARTMENT OF HOMELAND SECURITY'S R&D BUDGET PRIORITIES FOR FISCAL YEAR 2008

THURSDAY, MARCH 8, 2007

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION,
COMMITTEE ON SCIENCE AND TECHNOLOGY,
Washington, DC.

The Subcommittee met, pursuant to call, at 10:00 a.m., in Room 2318 of the Rayburn House Office Building, Hon. David Wu [Chairman of the Subcommittee] presiding.

BART GORDON, TENNESSEE
CHAIRMAN

RALPH M. HALL, TEXAS
RANKING MEMBER

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE AND TECHNOLOGY
SUITE 2320 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6301
(202) 225-6375
TTY: (202) 226-4410
http://science.house.gov

The Subcommittee on Technology and Innovation

Hearing on:

"The Department of Homeland Security's R&D Budget Priorities for Fiscal Year 2008 (FY08) "

2318 Rayburn House Office Building
Washington, D.C.

Thursday, March 8th, 2007
10:00 am – 12:00 pm

WITNESS LIST

The Honorable Jay M. Cohen
Under Secretary of Science and Technology
U.S. Department of Homeland Security

Mr. Vayl Oxford
Director of the Domestic Nuclear Detection Office
U.S. Department of Homeland Security

Dr. Gerald L. Epstein
Senior Fellow for Science and Security, Homeland Security Program
Center for Strategic and International Studies

Mr. Jonah J. Czerwinski
Senior Fellow, Global Leadership Institute
IBM

Ms. Marilyn Ward
Executive Director
National Public Safety Telecommunications Council

HEARING CHARTER

SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION
COMMITTEE ON SCIENCE AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES

The Department of Homeland Security's R&D Budget Priorities for Fiscal Year 2008

THURSDAY, MARCH 8, 2007
10:00 A.M.–12:00 P.M.
2318 RAYBURN HOUSE OFFICE BUILDING

1. Purpose

On Thursday, March 8, the Subcommittee on Technology and Innovation of the Committee on Science and Technology will hold a hearing to consider the President's fiscal year 2008 (FY 08) budget request for research and development at the Department of Homeland Security. Agency officials and outside observers will comment on budget priorities within the Science and Technology Directorate (S&T) and the Domestic Nuclear Detection Office (DNDO).

2. Witnesses

The Honorable Jay M. Cohen (R.Adm., USN ret.) is the Under Secretary of Science and Technology at the Department of Homeland Security (DHS).

Mr. Vayl Oxford is the Director of the Domestic Nuclear Detection Office (DNDO) at DHS.

Dr. Gerald L. Epstein is the senior fellow for science and security in the Homeland Security Program at the Center for Strategic and International Studies (CSIS).

Mr. Jonah J. Czerwinski is a senior fellow with the Global Leadership Initiative at IBM. He is also a Senior Advisor for Homeland Security Projects at the Center for the Study of the Presidency (CSP).

Ms. Marilyn Ward (minority witness) is Executive Director of the National Public Safety Telecommunications Council (NPSTC).

3. Brief Overview

- The FY 2008 budget request for the Department of Homeland Security's Science and Technology Directorate (S&T) is $799.1 million. This is a $90.1 million (9.5 percent) decrease from the FY 2007 enacted funding.
- The FY 2008 budget request for the Domestic Nuclear Detection Office (DNDO) is $569.1 million. This is an $80.9 million (17 percent) increase over the FY 2007 enacted funding. The bulk of the increase is for research, development, operations and systems acquisition.
- The S&T Directorate was reorganized into discipline-oriented divisions in mid-2006. While the FY 2008 budget request clarifies priorities among disciplines, there remains a question of whether DHS' R&D portfolio is properly balanced. The bulk of R&D funding goes towards biological and nuclear detection research. It is unclear if these priorities are in response to recognized risks or based on a completed risk assessment.
- There is a problematic lack of balance between basic and applied research and development. DHS dedicates the majority (52 percent) of its R&D funding to "product transition" (short-term development), while allocating only 11 percent to applied research and 13 percent to basic research. The remainder funds operational activities. De-emphasizing longer-term basic and applied research may curtail the ability of DHS to react to emerging and future threats.

4. Background

Research and development at the Department of Homeland Security is concentrated in the Science and Technology (S&T) Directorate and Domestic Nuclear Detection Office (DNDO). The S&T Directorate has responsibility for carrying out or coordinating nearly all federal homeland security related research. DNDO was separated from S&T in 2005 to specifically coordinate all research, development, and operations of technology to detect and report unauthorized transportation of nuclear and radiological materials.

S&T Directorate Organization

The S&T Directorate was reorganized into six divisions by Under Secretary Jay Cohen in mid-2006. The discipline-oriented divisions are intended to reflect specific threats to public safety and critical infrastructure. They include:

- Chemical and Biological: detection and mitigation of chemical and biological weapons threats
- Explosives: detection of and response to conventional (non-nuclear) explosives
- Human Factors: social science research to improve detection, analysis, and understanding of threats posed by individuals as well as how communities respond to disasters
- Infrastructure and Geophysical: identifies and mitigates threats to critical infrastructure
- Border and Maritime: develops technologies for surveillance and monitoring of land and maritime borders
- Command, Control, and Inter-operability: research and development support for inter-operable communications and cyber security

In addition to the six independent divisions, three offices coordinate the Directorate's R&D activities with extramural researchers and technology customers (typically other Directorates of DHS) and facilitate technology transfer. As part of the extramural research portfolio, the S&T Directorate funds the University Centers of Excellence program, which supports research across a broad variety of homeland security-related topics at university-based centers across the country.

DNDO Organization

DNDO was created to coordinate federal efforts to detect and respond to unauthorized transportation of nuclear or radiological materials into and within the United States. DNDO, which reports directly to the Secretary of Homeland Security, was transferred from the S&T Directorate in 2005. DNDO is responsible for coordination of federal agency efforts at DHS, the Department of Defense (DOD), the Department of Energy (DOE), the Federal Bureau of Investigations (FBI), the Nuclear Regulatory Commission (NRC), and the State Department to prevent the transport of nuclear and radiological materials across U.S. borders. It also works with international partners on detection and interdiction activities.

DNDO is responsible for research, development, testing and evaluation of detection technologies; acquisition of detection technologies; threat assessments; and technical support and training for State, local, and Federal Government partners and first responders. In 2006, DNDO completed a catalog of currently deployed global nuclear detection assets and an assessment of current detection capabilities, including an analysis of capability gaps across federal agencies.

5. FY 2008 Budget Request

S&T Directorate

In FY 2008, requested funding for the Science and Technology Directorate is cut by $174M or 17.8 percent to $799.1 million. (TABLE 1) As in previous years, the request is strongly weighted towards biological and chemical countermeasures research. This division represents 29 percent of the overall Directorate budget. Other priorities include research into explosives detection and mitigation, which represents eight percent of the overall budget; and command, control, and inter-operability, which also represents eight percent.

TABLE 1: Department of Homeland Security Science and Technology Directorate Budget
dollars in millions

Budget category	FY 2006 Enacted [1]	FY 2007 Enacted	FY 2008 Request	$ change/ FY 2007-08	Percent of total
Management and Administration	80.3	135.0	142.6	+7.6	17.8
Border and Maritime	43.3	33.4	25.9	-7.5	3.2
Chemical and Biological	387.0	313.5	228.9	-84.6	28.6
Command, Control, and Interoperability (C2I)	108.1	62.6	63.6	+0.99	8.0
Explosives	261.5	105.2	63.7	-41.5	8.0
Human Factors	6.4	6.8	12.6	+5.8	1.6
Infrastructure and Geophysical	86.1	74.8	24.0	-50.8	3.0
Innovation	0	38.0	59.9	+21.9	7.5
Laboratory Facilities	83.2	105.6	88.8	-16.8	11.1
Test, Evaluation, and Standards	34.6	25.4	25.5	+0.09	3.2
Transition	19.2	24.0	24.7	+0.7	3.1
University Programs	62.4	48.6	38.7	-9.9	4.8
TOTAL	**1487.0** [2]	**973.1**	**799.1**	**-174.0**	**100**

[1] Including 1 percent recission.
[2] Includes funding for Domestic Nuclear Detection Office (DNDO) which received separate appropriations in FY 2007.
(Source: Department of Homeland Security FY 2008 Budget Request)

The S&T Directorate also categorizes its research by timeline, defining "product transition" as short-term (0–3 years) development; innovative capabilities as mid-term (2–5 years) high-risk, high-payoff applied research; and "basic research" as long-term (>8 years), high-risk fundamental science. The remainder of the portfolio, including testing and standards, laboratory operations, and policy work is classified as "other." The FY 2008 budget strongly favors short-term development (TABLE 2), with just over 10 percent of funding dedicated to basic research. The balance of research funding is overseen by the Office of the Director of Research, which is also responsible for integrating internal and external basic research into DHS missions and S&T Directorate divisions.

TABLE 2: S&T Directorate Short and Long Term Research by Division
Percentage of overall division budget

Division	Basic (FY 07)	Innovative (FY 07)	Transition (FY 07)	Other (FY 07)	Basic (FY 08)	Innovative (FY 08)	Transition (FY 08)	Other (FY 08)
Borders and Maritime	6%	18%	71%	4%	5%	36%	57%	3%
Chemical and Biological	9%	3%	56%	32%	9%	4%	72%	15%
Command, Control and Inter-operability	11%	5%	60%	24%	12%	5%	72%	11%
Explosives	11%	5%	48%	36%	14%	11%	67%	7%
Infrastructure and Geophysical	18%	18%	31%	34%	26%	38%	22%	14%
Human Factors	41%	40%	4%	14%	33%	36%	20%	11%

(Source: Department of Homeland Security)

Within the S&T Directorate, the Administration requests reduced funding for nearly every division, with the only increases going to the relatively small Human Factors division and a nearly flat budget for the Command, Control, and Inter-operability division. Additionally, funding is cut significantly for University programs. A summary of some the major division and office budgets follows:

Innovation

A significant funding increase is provided to the Office of Innovation, which manages the Homeland Security Advanced Research Projects Agency (HSARPA) grant program. However, the funding increase will mainly support advanced technology development and demonstrations and does not provide funding for the basic and ap-

plied research priorities included in HSARPA's mandate. Additionally, $7.5 million of the total $59.9 million is budgeted for the Scalable Composite Vessel Prototype, a project to develop an improved hull for Coast Guard skippers.

Chemical and Biological

Funding for R&D in this division stayed flat, but $84.1M in funding was transferred to the new Office of Health Affairs for the operational (non-R&D) components of three programs (BioWatch, the Biological Warning and Incident Characterization (BWIC) system, and the Rapidly Deployable Chemical Detection System) which monitor for releases of biological or chemical weapons. The remaining budget will support R&D for the next generation of BioWatch, which is a monitoring program for detecting release of biohazards. This division represents by far the largest budget priority in the S&T Directorate.

Command, Control, and Inter-operability (C2I)

Funding for C2I stayed relatively flat from FY 2007, but follows a 41 percent reduction from FY 2006. This division covers research into cyber security, communications inter-operability, surveillance and investigative technologies, and threat assessment. In FY 2007, funding was cut for the emergent and prototypical technologies and rapid prototyping portfolios in this division, which limited the DHS' ability to address threats outside the existing divisions, perform basic research to identify vulnerabilities and countermeasures, and quickly address DHS-specific requirements for technologies.

Explosives

Funding for the explosives portfolio is reduced by $41.5 million or 40 percent from FY 2007 to $63.7 million. A portion of this reduction in funding is a result of the completion of the Counter-MANPADS program, which developed an airplane based defense against shoulder-fired missiles. If the Counter-MANPADS program is not considered in the budget calculation, the total funding for explosives countermeasures is decreased from $86.6M to $63.7M, a reduction of $22.9 million or 26.4 percent.

Testing, Evaluation, and Standards

The requested funding for this division is $25.5 million, which is relatively flat compared to FY 2007. This division is responsible for activities that include coordinating the development of metrics for equipment performance and certification, protocols for testing and training, and evaluation of equipment.

University Programs

Funding for University Programs is reduced by $9.9 million (20 percent) from FY 2007 to $38.7 million. The S&T Directorate plans to establish four new University Centers of Excellence—in spite of the reduced funding—and improve the capabilities of Minority Serving Institutions (MSIs) to conduct research in homeland security related areas and incorporate MSIs into the University Centers program.

DNDO

In FY 2008, the Administration requests $561.9 million for DNDO (TABLE 3). This request increases total funding for the Office by $80.9 million or 17 percent. The budget is increased for every component of DNDO, with the bulk of the increase going towards Research, Development, and Operations and Systems Acquisition.

TABLE 3: Department of Homeland Security Domestic Nuclear Detection Office Budget

dollars in millions

Budget Category	FY 2006 enacted	FY 2007 enacted	FY 2008 request	$ change/ FY 2007-08
Management and Administration	2.5	30.5	34.0	+3.5
Research, Development, and Operations	189.8	272.5	319.9	+47.4
Systems Acquisition	125.0	178.0	208.0	+30.0
TOTAL	**317.4**	**481.0**	**561.9**	**+80.9**

(Source: Department of Homeland Security FY 2008 Budget Request)

A summary of the major categories follows:

Management and Administration

The $3.5 million increase for Management and Administration provides reimbursement to other federal agencies providing staff members to DNDO as detailees and goes toward creating additional full-time positions. Many of these staff support research, development, and operations activities and aviation and maritime security activities. A larger full-time, non-detailee staff will improve DNDO's ability to conduct testing and evaluation and support improved acquisition protocols that will result in use of better detection technology.

Research, Development, and Operations (RD&O)

Research, development, and operations (RD&O) activities within DNDO include engineering and architecture for detection systems, high-risk transformational R&D, technology assessments, operations support for government partners, and the National Technical Nuclear Forensics Center. Together, these components aim to support a seamless system of nuclear detection from basic research through technology development and implementation. The requested funding increase of $47.4 million or 17 percent will go primarily to transformational research and development (up $22.9 million or 30 percent).

Within the transformational R&D portfolio, the FY 2008 priority will be the initiation of several Advanced Technology Demonstrations (ATDs). For example, one of the ATDs will focus on radioactive material detection in various transit systems such as ship or airplane transit. Other priorities will be port security, training for State and local law enforcement, and assessing hand-held detection technologies.

Systems Acquisition

The budget request for systems acquisition activities of $208 million includes funding for deploying radiation monitors at ports of entry and the Securing the Cities Initiative, which is a program to deploy nuclear detection equipment at entryways into a city, including ports, highways, and airports. New York City was the pilot city in 2006, and the Administration requests funding in FY 2008 to expand the program. The requested $30 million (17 percent) increase in funding for Systems Acquisition will go entirely toward this second phase of the Securing the Cities Initiative.

6. Issues and Concerns

How does the Department of Homeland Security use risk assessments to determine R&D priorities? The budget request for R&D at DHS raises a number of concerns, some of which are ongoing from the inception of the Department. The Department's mission is to reduce the vulnerability of the United States to—and mitigate the effects of—threats, both manmade and natural, but the overall justification of the DHS R&D portfolio makes no indication that there was any threat used to inform how research areas were prioritized. The S&T Directorate plans to issue a five-year strategic plan in April 2007 that will include some input from the Homeland Security Institute, a policy advisory board, on risk. The lack of investment in risk assessment is wasteful at best and potentially dangerous, as there is no basis for prioritizing unexpectedly urgent threats. In one example cited by the Under Secretary, following the liquid explosives threat to airplanes in August 2006, it took the S&T Directorate two months to set up a research program to evaluate the risks of and countermeasures against liquid explosives. This delay hampered the ability of the Transportation Security Administration (TSA) to develop guidelines for transporting liquids on planes, causing countless delays and problems for travelers and airlines.

Is the balance between short- and long-term research at DHS appropriate? What criteria does DHS use to determine the balance between long- and short-term research? While the requested funding for basic research within DHS S&T has more than doubled from FY 2007 to approximately 13 percent in FY 2008, the Department's R&D portfolio remains strongly weighted towards end-stage technology development with funding for basic research well below the Under Secretary's goal of 20 percent of all research dollars. Likewise, DNDO does not give adequate priority to basic research, requesting $100 million for transformational R&D but only directing 11 percent ($11.1 million) of that funding to basic research. The remainder funds technology development.

The large proposed cuts to the University Centers of Excellence program further reduce investment in basic research. Funding for emergent and prototypical technologies, cut significantly in FY 2007, also remains low. Emphasizing short-term research makes the Department significantly less agile and responsive, locking it into a single technological response to emerging and future threats.

How do DHS R&D priorities reflect the needs of customers, including other Directorates within DHS, interagency partners, and State and local governments? Under Secretary Cohen has said that the research priorities of the S&T Directorate should directly serve "customers"—defined as users of DHS' research results and developed technologies. To that effect, the Under Secretary established "integrated product teams" comprised of officials from other DHS components who advise the S&T Directorate on their technology needs, thus informing specific research priorities. While these interdisciplinary teams are a step in the right direction, the Department needs a much stronger focus on integrating the opinions of interagency and outside partners. At least 10 agencies, including the National Institute of Standards and Technology (NIST), the National Science Foundation (NSF), the Department of Transportation (DOT) and others perform homeland security-related R&D. However, there is no formal mechanism for leveraging the R&D work of other agencies within DHS. Both the S&T Directorate and DNDO have been criticized for ignoring the work and advice of other federal agencies. Similarly, State and local officials, including first responders, have complained that DHS is not responsive to their requests and recommendations related to technology development. The Department must development a formal mechanism for responding to the final users of the R&D it supports.

Chairman WU. I would like to call the Subcommittee to order. We want to welcome everyone to this morning's hearing on the fiscal year 2008 Research and Development budget for the Department of Homeland Security. I want to offer a special welcome to Under Secretary Jay Cohen, who joined the Department of Homeland Security's Science and Technology Directorate in August, 2006. Your reputation as a problem-solver precedes you from the Office of Naval Research.

I also want to welcome our other witnesses, who represent a valuable pool of expertise across Homeland Security related topics. Mr. Vayl Oxford is the Director of the Domestic Nuclear Detection Office at the Department of Homeland Security. Prior to his appointment at DNDO, Mr. Oxford served as the Director for Counter Proliferation at the National Security Council.

Dr. Gerald Epstein is a senior fellow for Science and Security for Homeland Security at the Center for Strategic and International Studies. He has served at the Institute for Defense Analysis and with the White House Office of Science and Technology Policy.

Mr. Jonah Czerwinski is a senior fellow for Homeland Security with IBM's Global Leadership Initiative. He is also a senior advisor for Homeland Security projects at the Center for the Study of the Presidency.

Ms. Marilyn Ward is the Executive Director of the National Public Safety Telecommunications Council; Representative Gingrey will tell us a little more about her background in a moment.

We look forward to hearing your thoughts on how to support a world class R&D enterprise at the Department of Homeland Security that keeps our communities safe.

When the Science Committee helped write the legislation authorizing the R&D Programs at DHS, we envisioned an organization that would support the Science and Technology needs of people on the front lines of domestic security; from first responders to computer security professionals, from medical workers to civil engineers. Frankly, it has been a bit of a rough start. We are familiar with management problems that have caused a lack of focus on important R&D priorities and the attrition of some of the best and brightest minds from the S&T Directorate.

I have also heard some concerns from communities and cities and users of some of the DHS technology, which feel that DHS R&D Programs at the S&T Directorate and at DNDO have not been entirely responsive to their needs.

But I do remain hopeful. Under Secretary Cohen has launched an ambitious new management structure to insure a more cohesive S&T Directorate. Hopefully the R&D results will flow smoothly from the earliest research concepts to the most advanced technology development. Only time will tell.

Under Secretary Cohen has admirably acknowledged the problems within the S&T Directorate which is the first step in formulating solutions. This committee stands ready to work with all of you and your staffs to insure that we have a strong and responsive research operation at DHS.

I am concerned, though, about the lack of a strategic plan based on risk assessment that should be the basis for research priorities within DHS. We can fund billions of dollars in research, but if we

don't pay attention to the risks we should be addressing, we won't have the answers we need when we need them. We can base research on anecdotal impressions of need, but that is not the scientific approach that the American people have a right to expect.

I strongly encourage you to carry out a detailed, systematic, scientific risk assessment soon so that we know whether our investments are in the right place. Nuclear threats will obviously be a major part of any threat assessment. I am especially eager to see signs of close cooperation between the S&T Directorate and the DNDO. It is imperative that you all take advantage of the complementary efforts of your offices and avoid duplication.

I am committed to working with the Department to insure that our R&D efforts there are successful in increasing our knowledge of how to confront catastrophes, whether from human or nature causes.

I look forward to hearing all of the witnesses' thoughts on the fiscal year 2008 budget request and how that budget supports science and technology to make our nation safer.

I now want to recognize my colleague and the Ranking Member from Georgia, Dr. Gingrey, for his opening remarks.

[The prepared statement of Chairman Wu follows:]

PREPARED STATEMENT OF CHAIRMAN DAVID WU

I would like to call the Subcommittee to order.

I want to welcome everyone to this morning's hearing on the FY08 research and development budget for the Department of Homeland Security. I want to offer a special welcome to Under Secretary Jay Cohen, who joined the Department of Homeland Security's Science and Technology Directorate in August 2006. Your reputation as a problem-solver precedes you from the Office of Naval Research. I also want to welcome our other witnesses, who represent a valuable pool of expertise across homeland security-related topics. Mr. Vayl Oxford is the Director of the Domestic Nuclear Detection Office at the Department of Homeland Security. Prior to his appointment to DNDO, Mr. Oxford served as the Director for Counter-proliferation at the National Security Council. Dr. Gerald Epstein is a senior fellow for science and security in the Homeland Security Program at the Center for Strategic and International Studies. He has served at the Institute for Defense Analyses, and with the White House Office of Science and Technology Policy. Mr. Jonah Czerwinski is a Senior Fellow for Homeland Security with IBM's Global Leadership Initiative. He is also a Senior Advisor for Homeland Security Projects at the Center for the Study of the Presidency. Ms. Marilyn Ward is the Executive Director of the National Public Safety Telecommunications Council. Representative Gingrey will tell us a little more about her background in a moment.

We look forward to hearing your thoughts on how to support a world-class R&D enterprise at the Department of Homeland Security that helps keep our communities safe.

When the Science Committee helped write the legislation authorizing the R&D programs at DHS, we envisioned an organization that would support the science and technology needs of people on the front lines of domestic security—from first responders to computer security professionals, from medical workers to civil engineers. Frankly, it's been a rough start. We're familiar with management problems that have caused a lack of focus on important R&D priorities and the attrition of the best and the brightest minds from the S&T Directorate. I've also heard from communities and cities which feel that DHS R&D programs at the S&T Directorate and the Domestic Nuclear Detection Office (DNDO) have not been entirely responsive to their needs.

But I remain hopeful. Under Secretary Cohen has launched an ambitious new management structure to ensure a more cohesive S&T Directorate. Hopefully, the R&D results will flow smoothly from the earliest research concepts to the most advanced technology development. Only time will tell whether the changes Under Secretary Cohen has made will bring about the radical improvements to the S&T Directorate that our nation needs. Under Secretary Cohen has admirably acknowledged the problems within the S&T Directorate, which is the first step in developing a so-

lution. This committee stands ready to work with Under Secretary Cohen and all of his staff to ensure that we have a strong and responsive S&T Directorate.

I am concerned though about the lack of a strategic plan or risk assessment that should be the basis for research priorities within the Department of Homeland Security. We can fund billions of dollars in research, but if we don't pay attention to the risks we should be addressing, we won't have the answers we need when we need them. We can base research on anecdotal impressions of need, but that is not the scientific approach that the American people have a right to expect. I strongly encourage you to carry out a detailed, scientific risk assessment soon, so that we know whether our investments are in the right place. Nuclear threats will obviously be a major part of any threat assessment. I am especially eager to see signs of close cooperation between the S&T Directorate and Domestic Nuclear Detection Office. It is imperative that you take advantage of the complementary efforts of your offices and avoid duplication.

I am committed to working with the Department of Homeland Security to ensure that R&D investments are successful in increasing our knowledge of how to confront catastrophes, whether from human or natural causes. I look forward to hearing all of the witnesses' thoughts on the FY08 budget request and how that budget supports science and technology to make our nation safer.

I now want to recognize my colleague and the Ranking Member from Georgia, Dr. Gingrey, for his opening remarks.

Mr. GINGREY. Mr. Chairman, thank you and in the interest of full disclosure I want to say that I do know Dan Quayle, and I am a lot like him. I can't spell tomato or potato, and I don't know if I could give the best impersonation of him like my colleague did of President Clinton, but if I stumble, forgive me. It is my staff. They gave me remarks that are written in very small type, and I will talk to them about that later.

Great to be with my Chairman this morning at this important hearing. I want to thank him for holding the hearing on science and technology developments at the Department of Homeland Security, and also a special thank you to our esteemed panel of witnesses, taking time to dialogue with us about the role that science and technology is playing in securing our nation.

Mr. Chairman, I strongly believe our nation's scientific enterprise remains a critical component of national security. The efforts of the Science and Technology Directorate and the Domestic Nuclear Detection Office contribute to the preparedness of our nation against terrorism and nuclear disasters. These organizations tap into the limitless creativity of our nation's scientists and engineers to bring cutting-edge technology to those defending our nation, from servicemen and women to border patrol agents and first responders.

I am particularly pleased to welcome Under Secretary Cohen and Mr. Vayl Oxford to this subcommittee hearing. Gentlemen, your service to our great nation is greatly appreciated. I very much enjoyed meeting both of you earlier this week. That was my pleasure, and I look forward to continuing the conversations we started in regards to the exciting opportunities that scientific research is providing to securing our homeland. This committee is committed to supporting your work and helping you create both a balanced and innovative research portfolio.

And I would like to take this opportunity to thank Ms. Marilyn Ward for joining us today to take part in this discussion. Ms. Ward's organization, the National Public Safety Telecommunications Council, includes representatives from many different first responder communities. Such representatives include the International Association of Chiefs of Police, emergency managers, as well as fire chiefs. Ms. Ward, I look forward to hearing from you

on how the Department's research and the development activities can further support our nation's first responders.

In particular, your appearance will allow us to examine one highly-influential program in the Science and Technology Directorate, and that is the Office for Inter-operable Communications, and I know you will tell us about that. This office has worked for the last several years with first responders to improve the inter-operability of communication equipment, and that work continues today in cooperation with the new Office of Emergency Communications within DHS Preparedness Directorate.

I am eager to not only hear from our witnesses how Science and Technology efforts save or are yielding immediate benefits to the defense of our nation but also ways we can improve upon your efforts. The President has requested over $1.3 billion in funding for the two organizations before us today for this next '08 fiscal year. How that funding is allocated across the various programs and projects in your organization no doubt is a difficult task, considering the reality of the world that we now live in. Whether the greatest threat to our country is a radiologic device coming through our ports or an infectious disease outbreak or a cyber attack on our nation's financial infrastructure, the fundamental challenges before us how to best distribute the limited funding in the face of these highly-uncertain and varied threats.

In addition to prioritizing these various threats our country now faces, we must also consider the nature of research performed to combat them. Do we focus federal spending towards long-term basic research? What percentage of the funding do we allocate towards incremental improvements to our current capabilities? With these overarching questions in mind, I look forward to delving more deeply into the activities of Science and Technology Directorate and the Domestic Nuclear Detection Office.

I once again thank all of the witnesses for taking the time to be here with us today. I anticipate this hearing will yield a fruitful and productive conversation. Mr. Chairman, I look forward to hearing from them and continuing to work with you on this very important subcommittee, and with that I will yield back to the Chairman.

[The prepared statement of Mr. Gingrey follows:]

PREPARED STATEMENT OF REPRESENTATIVE PHIL GINGREY

I first want to thank Chairman Wu for holding this critically important hearing on the science and technology developments at the Department of Homeland Security. Also, a special thank you to our esteemed panel of witnesses for taking time to dialogue with us about the role science and technology is playing in securing our nation.

Mr. Chairman, I strongly believe our nation's scientific enterprise remains a critical component of homeland security. The efforts of the Science and Technology Directorate and the Domestic Nuclear Detection Office contribute to the preparedness of our nation against terrorism and natural disasters. These organizations tap into the limitless creativity of our nation's scientists and engineers to bring cutting edge technology to those defending our nation from servicemen and women to border patrol agents to first responders.

I'm particularly pleased to welcome Admiral Cohen and Mr. Vayl Oxford to this subcommittee hearing. Gentlemen your service to our great nation is greatly appreciated and I very much enjoyed meeting with you both this week. I look forward to continuing the conversations we started in regards to the exciting opportunities scientific research is providing to the securing of our homeland. This committee is

committed to supporting your work and helping you create both a balanced and innovative research portfolio.

I would like to take this opportunity to thank Ms. Marilyn Ward for joining us today to take part in this discussion. Ms. Ward's organization, the National Public Safety Telecommunications Council includes representatives from many different first responder communities. Such representatives include the International Associations of Chiefs of Police, emergency managers, as well as fire chiefs. Ms. Ward, I look forward to hearing from you on how the Department's research and development activities can further support our nation's first responders. In particular, your appearance will allow us to examine one highly influential program in the Science and Technology Directorate, the Office for Inter-operable Communications. This office has worked for the last several years with first-responders to improve the interoperability of communications equipment and that work continues today in cooperation with the new Office of Emergency Communication within the DHS Preparedness Directorate.

I am eager to not only hear from our witnesses how science and technology efforts are yielding immediate benefits to the defense of our nation, but also ways we can improve upon these efforts.

The President has requested over $1.3 billion dollars in funding for the two organizations before us today for fiscal year 2008. How that funding is allocated across the various programs and projects in your organizations, I have no doubt, is a difficult task considering the reality of the world we now live in. Whether the greatest threat to our country is a radiological device coming through our ports, or an infectious disease outbreak, or a cyber attack on our nation's financial infrastructure; the fundamental challenge before us is how to best distribute limited funding in the face of these highly uncertain and varied threats.

In addition to prioritizing these various threats our country now faces, we must also consider the nature of research performed to combat them. Do we focus federal spending towards long-term, basic research? What percentage of funding do we allocate towards incremental improvements to current capabilities?

With these overarching questions in mind, I look forward to delving more deeply into the activities of the Science and Technology Directorate and the Domestic Nuclear Detection Office. I once again thank all the witnesses for taking the time to be here today and anticipate this hearing will yield a fruitful and productive conversation. Mr. Chairman, I look forward to continuing to work with you on this subcommittee, and with that I yield back the balance of my time.

Chairman WU. Thank you, Dr. Gingrey. Other Members who wish to submit opening statements, the opening statements will be added to the record.

[The prepared statement of Mr. Mitchell follows:]

PREPARED STATEMENT OF REPRESENTATIVE HARRY E. MITCHELL

Thank you Mr. Chairman.

As you know, we have a problem in Arizona. Our border is broken and the Federal Government is failing to fix it. The border is porous, and monitoring is inadequate. We have deployed systems and technology to help, but not nearly enough to stem the flow of illegal immigrants, drugs and threats of terrorism.

We should be investing in border-related research and development, but unfortunately, the budget proposal before us today, seeks cuts.

This just doesn't make any sense. Not for Arizona, and not for our country.

Budgeting is about priorities, and I believe our priorities should be based on solid risk assessment. Unfortunately, it doesn't look like today's proposal does that.

Clearly biological and nuclear threats deserve our attention, but so do University Centers for Excellence and much of the long-term research and development that our Federal Government undertakes to protect us from future risks. Not to mention the border.

I look forward today's testimony.

I yield back the balance of my time.

Chairman WU. And I now turn to our witnesses. As each of you all already know, please try to keep your testimony to within approximately five minutes or so, summarizing your substantial written testimony. And after your testimony the Members of the Committee will have a rotating period of five minutes each to ask questions. And we will start with Under Secretary Cohen.

STATEMENT OF MR. JAY M. COHEN, UNDER SECRETARY OF SCIENCE AND TECHNOLOGY, DEPARTMENT OF HOMELAND SECURITY

Mr. COHEN. Good morning, Chairman Wu, Congressman Gingrey, and Congressman Bonner. I can tell you it is a personal honor to appear before the distinguished Science Committee, and I have had the opportunity to testify in the past. I note that both the chairman and the Ranking Member went to medical school, so you will appreciate I may limit my comments here.

Chairman WU. One of us finished, one of us didn't. Since his title is doctor, you can take your guess.

Mr. COHEN. Well, I won't venture——

Chairman WU. The one that didn't finish went on to become a rich man.

Mr. COHEN. Yes, sir.

Chairman WU. And the other one is struggling.

Mr. COHEN. I won't venture to guess who is smarter. And I am also humbled to be sitting in a panel with such distinguished individuals as are sitting before you. But I am here to update you on the progress that the Department of Homeland Security Science and Technology Directorate has made and discuss the President's budget request for fiscal year 2008, and how I believe it will position us to develop and transition technology to protect the Nation from catastrophic events as the Congress and the Administration wisely envisioned in the 19 pages of enabling legislation for the Department of Homeland Security.

As the Chairman has already indicated, my directorate is committed to serving our customers. Those are the 22 DHS components and their customers, the customers of my customers, our heroes, the first responders, the police, fire, and EMT. But the customers as customers are greater than that. For the Coast Guard, they are the guardsmen who sail in harm's way, for the Border Patrol, the agents who man the border, and for the TSA, the screeners. They are the hardworking men and women on the front lines of Homeland Security, and they appreciate your support, and in prior testimony I commented on Chairman Bennie Thompson's very kind e-mail to those many hardworking people, appreciating what they have done.

I greatly appreciate the support and the leadership of the Congress. Last year you took a very hard and strong decision in September to restore the fiscal year 2007 funding. That has been enormously helpful to me in kick starting the directorate to achieve the results that we all desire, and I am especially grateful of that in what I know is a difficult election year. So thank you so much.

And I also want to thank the staff, special staff of the Science and Technology Committee, but all the staffs of the committees that I work with who have worked with me, have tried to educate me, and it is a very professional relationship. And I congratulate you both on the selection of the new staff for the Science and Technology Committee.

As you are aware, the focus of my first months on the job have been laying the foundation to align the directorate for success, and that was to excel in four key areas, and I shared this with you last September when I testified previously. It was to get the organiza-

tion, the people, the books, and the content of the program right. Those were my four gets. But they were focused on the threats as you mentioned, Mr. Chairman, and the threats as I defined them simplistically were bombs, borders, bugs, and business. And bombs, borders, and bugs we can all feel, we can all sense. They are tangible, but the business is really about the cyber backbone that enables this incredible technology-focused economy that we have. And if the bad guys that you have mentioned can take that away from us, we will have as much panic as I believe we would from a nuclear device.

I believe the record will show that we made good progress in my first six months on the job in all of these areas and just to give a quick highlight, we have, in fact, with the approval of the Congress and Secretary Chertoff in the first month realigned the directorate. I have a strong leadership team in place where all the key positions are filled. We have welcomed over 20 new highly-qualified scientists and engineers, subject-matter experts, and professionals into the directorate, and four Government Service personnel who left the directorate last spring have asked to come back and are now back on board, and welcome them and the continuity that they bring.

I am basically two-thirds manned of where I need to be by the end of this fiscal year and we are making very good progress. I have no shortage of volunteers. Even some who want to work pro bono I am trying to figure out how I do that.

The six technical divisions are all led by veteran S&T members. My three research investment portfolio directors for research, basic research, transition, and innovation, my high risk, provide the crosscutting coordination amongst those six divisions so I don't end up with stovepipes.

And finally, those divisions are focused on what I believe you have mandated and the public expects are the high priority issues of explosives, things that go bang, of the nuclear radiological, that is Mr. Oxford, but we work closely together, chem bio, half of my budget, and it is a threat which I believe the other witnesses will indicate is as significant as the nuclear radiological threat in today's world. Command, control, and inter-operability, and I know you will ask more about that. Borders and maritime. I initially thought about that as two divisions, but our borders on the west coast are sea on the north land, sea on the southeastern land and the southwest, 48,000 border patrol, 40,000 Coast Guardsman. The synergies there are impressive. It is one division, but the comment of the Coast Guard has detailed an active duty Coast Guard captain to be my deputy director so we are seamless. And at the end of the day the more we can do to remove seams, the safer we will be against a terrorist.

We have established a division of human factors. Dow Chemical has a wonderful commercial today about the human element. It is hostile intent, the psychology of terrorism. These may be the light sciences, but they are critically important if we are going to defend the country. I came on board on the 10th of August. That was the day of the liquid explosives plot in England. The Brits did it right. They got the bomber. You get the bomber, you don't have to worry about the bomb, but regrettably, there may always be leakage, so

we do worry about the bomb. But human factors, like command, control, and inter-operability, crosscut.

And finally, infrastructure protection and geophysical sciences. I am responsible, as you have noted, for all hazards, not just man-made. And so tsunamis, hurricanes, fire, flooding, earthquakes, we have got to do a better job of protecting against those.

Now, there is much more I could say, but I will reserve that for the question and answer period. I did want to note a statement that I have been making. Chairman Wu, I know I finally arrived because I am in a blog now, last Friday, when I said that we are in crisis in science and technology. In the middle schools, kids are turning away from math and science. You know this better than I do. And Congressman Bonner, I was so pleased to see Governor Riley's State of State Address, where he devoted nearly half of his message, and we are seeing that in so many states; Kentucky, and there were hearings yesterday on the Hill. But we are in crisis, and if we don't get the kids to take the hard subjects of science and math, we will not enjoy the economic society, the technological dominance that we have enjoyed for so long. And so I compared it to the Play Station society or the Play Station generation, and some people viewed that as derogatory, but I stand by those remarks. And we want instant gratification, but science and technology require much more.

So we are moving forward on Centers of Excellence. We currently have seven. We are realigning them to be in line with my divisions. We have broad agency announcements out for an additional four to meet the needs that we weren't meeting, and I am allotting my very robust thanks to you, Scholarship and Fellowship Program, to those Centers of Excellence, which currently include over 80 universities and colleges in the states but shortly will include more than 100. This is exciting. The S&T Directorate appreciates the many demands on the taxpayers' precious dollars. We are committed to being wise stewards of those public monies that you have and will entrust to us. I appreciate the Science and Technology Committee's support. I welcome your oversight, and I will be happy to take your questions. Thank you so much.

[The prepared statement of Mr. Cohen follows:]

PREPARED STATEMENT OF JAY M. COHEN

INTRODUCTION

Good Morning Chairman Wu, Ranking Member Gingrey, and distinguished Members of the Subcommittee. It is an honor to appear before you today to update you on the progress of the Department of Homeland Security's (DHS) realigned Science and Technology Directorate (S&T Directorate) and discuss how the Directorate's priorities in the President's Budget Request for Fiscal Year 2008 will position us to develop and transition technology to protect the Nation from catastrophic events.

The S&T Directorate is committed to serving our customers, the components that comprise the Department of Homeland Security—and their customers—the hard-working men and women on the front lines of homeland security, especially the first responders, who need ready access to technology and information to perform their jobs more efficiently and safely. I am honored and privileged to serve with the talented scientists, engineers and other professionals who support these dedicated Americans in our shared mission to secure our homeland and defend our freedoms.

First and foremost, I am very appreciative of the leadership of the Congress in its support of the S&T Directorate, and of me personally, as I assumed the role of Under Secretary for Science and Technology last August. The informed counsel of Committee Members with homeland security oversight, and that of their staffs, has

been invaluable to my efforts to position the S&T Directorate for accountability, tangible results and success, both for today and in the future.

Also, thank you for your vote of confidence in the Directorate, evidenced by the decision to appropriate $848 million in FY 2007. This has been enormously helpful in my efforts to better align people with our mission to develop a robust science and technology capability to protect the Nation as Congress envisioned in the enabling legislation for the Department. We look forward to working with the 110th Congress in a bipartisan and non-partisan manner to use science to better secure the Nation.

I am also grateful for the leadership of the President and Homeland Security Secretary Michael Chertoff and for the vision and guidance that the Secretary and Deputy Secretary Michael Jackson have contributed to the realignment process.

THE FIRST 180 DAYS—ALIGNED AND OPEN FOR BUSINESS

My first six months on the job have been focused on laying the foundation in organization, people, and processes to enable the Directorate to skillfully apply the resources you have wisely provided in ways that best serve the American people and better secure our homeland. I am pleased to report that we are "open for business," and your support of the President's FY 2008 Budget Request will allow us to build upon that momentum.

As I've said on many occasions, the S&T Directorate must excel in four key areas if we are to accomplish these goals: We must get the organization, the people, the books, and the program content right. These four "gets" are the cornerstones of the realignment effort and we've made significant progress in each of these areas. In addition to the four gets, the four Bs—bombs, borders, bugs and business—provide the thematic approach to help keep us focused on the priority areas for the S&T Directorate.

I have realigned the S&T Directorate to help it fulfill its potential of becoming the customer-focused, output-oriented, science and technology management organization that Congress intended it to be and the Nation deserves. I thank Congress for its support of the new organizational structure that, in turn, is supportive of a broad and balanced range of activities that are aimed at identifying, enabling and transitioning new capabilities to our customers to better protect the Nation. We have organized our program management into six technical divisions that are led by veteran S&T Directorate staff members and linked to three research and development investment portfolio directors in a "matrix management" structure. The technical divisions are focused on enduring homeland security disciplines of Explosives; Chemical and Biological; Command, Control & Inter-operability; Borders and Maritime Security; Human Factors; and Infrastructure Protection and Geophysical Sciences. The effort to combat the threat posed by nuclear or radiological weapons is primarily led by the Domestic Nuclear Detection Office. The portfolio directors—Director of Research, Director of Transition, and Director of Innovation/Homeland Security Advanced Research Projects Agency (HSARPA)—provide cross-cutting coordination of their respective aspects of the investment strategy within the technical divisions.

Office of the Under Secretary for Science & Technology

I am pleased to report that today the S&T Directorate has a strong leadership team in place with all key positions filled. Since August, we have also welcomed 20 new highly qualified subject matter experts and professionals to the S&T Directorate, including three former DHS S&T employees who had previously left the Directorate and who have returned. Overall, we are 66 percent staffed and plan to have 100 percent of staff in place by the end of 2007.

I have made significant strides in "getting the books right" by holding the S&T Directorate to a high standard of fiscal responsibility. Toward this end, I have established an Office of Strategy, Policy & Budget Division led by the S&T Chief Financial Officer that has put in place the systems and protocols that will enable the S&T Directorate to be fully responsive and transparent in the budget development process and in the sound fiscal management of S&T appropriations. This new office is enhancing the efficiency of S&T operations by integrating related functions of policy, planning, programming, budgeting and execution. Centralizing financial oversight has enabled the S&T Directorate to implement corrective actions to address financial management deficiencies and accelerate the distribution of funds to DHS Laboratories, Department of Energy (DOE) National Laboratories, private industry and academia. As a result, the S&T Directorate has committed approximately 50 percent of its FY 2007 budget compared to six percent at the same time last year, significantly accelerating the distribution of funds to DHS Labs, DOE Labs, industry and academia, which will result in accelerated technology development and delivery to keep our nation safer.

In other developments, I have added a director of Special Programs to work in select, mission-critical areas. And a new director of Test & Evaluation and Standards is building upon the S&T Directorate's previous work in homeland security standards and adding test and evaluation capabilities to advance this effort and draw greater industry participation in developing new technologies for homeland security applications throughout DHS. We have also established a Corporate Communications Office to inform and engage our customers and their customers in the S&T Directorate's broad investment portfolios.

I also know that we must look beyond our Department, indeed beyond our nation's borders, for solutions in combating domestic terrorism. Therefore, consistent with DHS enabling legislation, I have established Interagency and International Program Offices responsible for, respectively, coordinating with other Executive Branch agencies to reduce duplication and identify unmet needs, and coordinating our international outreach efforts to help us tap into science and technology commu-

nities across the globe for solutions to counter domestic terrorism. Embedded S&T Directorate liaisons in Europe, the Americas and Pacific/Asia are casting a wide global net to identify the most viable homeland security solutions and their providers. This office will allow S&T to benefit from and leverage off of the efforts of our allies in the War on Terror.

I have developed mechanisms in three areas to better coordinate the scientific research and technical development activities of the S&T Directorate with those of other federal Agencies.

First, our overarching policy is to leverage research and development efforts across the Federal Government to benefit our DHS customers as well as first responders. Our preference is to avoid replicating efforts underway by other federal agencies in favor of coordinating and collaborating with our federal counterparts in research areas of mutual interest and benefit. The *Homeland Security Act of 2002* provides me with specific authorities in this regard.

The second coordinating mechanism is aimed at better positioning the Directorate to increase our awareness of, and the opportunities to participate in or otherwise benefit from, other federal research, development, test and evaluation (RDT&E) efforts that are relevant to our mission. The new directors for Interagency Coordination and Special Programs report directly to me regarding their progress in this area.

The third mechanism for coordinating research and development (R&D) is through specific agreements and relationships. For example, in December of 2006, the Department of Defense (Homeland Defense), the Department of Justice, and DHS S&T signed a Memorandum of Agreement (MOA) to promote closer coordination and collaboration of our R&D and technology transfer efforts. The S&T Directorate is also actively engaged in various committees, subcommittees, and working groups of the National Science and Technology Council. In recent months, we have developed a closer working relationship with U.S. Northern Command, U.S. Joint Forces Command, the Technology Support Working Group, the National Guard Bureau, and the Joint IED Defeat Organization regarding research and development initiatives, defining their inter-operability requirements through established Defense Department, Joint, and military service-based processes as appropriate. In addition, S&T has established a pilot program and assigned a liaison official to the California Governor's Office of Homeland Security in Sacramento in an effort to recognize and address coordination and inter-operability issues early on.

Last December, we saw the "physical manifestation" of our restructuring plan spring to life with the relocation of 340 of our staff members within the Directorate. Staff are now physically co-located within their new organizational alignments. At the same time, I issued the first S&T Organization and Requirements Manual (STORM) that defines functions, duties and responsibilities for the administration and management of the Directorate. The STORM tells our customers who we are and how we function so they may better understand the capabilities we can bring to bear in support of their protective missions.

Throughout this process, it was very important to me personally that S&T staff be kept informed of our plans for the realignment and that they have a forum for asking questions and expressing their views and concerns. Since last August, I have held four "All Hands" meetings at regular intervals to brief all S&T staff, including teleconference links with staff in other locations such as the Transportation Security Laboratory in Atlantic City, Plum Island Animal Disease Center, and the Environmental Measurements Laboratory in New York City. These meetings also allow me to recognize the achievements of staff members, to answer questions and solicit input, and, most importantly, express my gratitude for their excellent work and for all the cooperation, support and patience they have exhibited during this transitional period.

During the first six months of my tenure as Under Secretary for Science and Technology, I have focused on building the organization, team and processes that are necessary for any science and technology management organization to succeed. While our effort to completely institutionalize these changes continue, we now have a foundation in place that allows us to focus on delivering products to our customers as we execute our FY 2007 appropriation. The S&T Directorate is striving to be effective, cost-efficient, responsive, agile and flexible, and with your support of the President's FY 2008 Budget Request we will build on our current momentum.

CUSTOMER/OUTPUT FOCUSED

The S&T Directorate functions as the science and technology manager within the Department. We invest in science and technology that supports DHS components in their efforts to protect our homeland against catastrophic events—technology that makes the Nation safer. In the last six months, we have established meaningful

working relationships with our DHS operational component customers. As they appear before you this year, I encourage you to ask them about the ways that S&T is addressing their operational needs. Thanks to the support of the Congress and the leadership of the Department, we are gaining significant momentum, and I humbly ask for your continued trust and support so that we can build on those efforts.

The S&T Directorate develops and manages an integrated program of science and technology, from basic research through technology transition to customers that are the operating components of DHS, State, local and tribal governments, first responders and private sector entities. The managers of this program are predominantly active scientists and engineers in the many disciplines relevant to Homeland Security. They are guided by a multi-tiered investment strategy and review process based on higher guidance, the stated needs of our customers, and technology opportunities.

S&T's three R&D portfolios support a broad range of program activities across the Directorate. The President's FY 2008 Budget Request includes $86 million for the basic research portfolio which addresses the long-term R&D needs for the Department in sciences of enduring relevance to Homeland Security. The transition portfolio, designed to provide mission-capability relevant technology in support of the Department's acquisition programs, is driven by customer needs through a DHS customer-led IPT process. The President has requested $343 million in FY 2008 for this effort. The Director of HSARPA administers the $73 million innovation portfolio (including the Small Business Innovation Research program) to promote revolutionary changes in technologies with a focus on prototyping and deploying technologies critical to homeland security. This portfolio, balanced around risk, cost, impact and time to delivery, produces capabilities of high technical quality responsive to homeland security requirements.

Product Transition (0-3 yrs)	**Innovative Capabilities (2-5 yrs)**
▪ Focused on delivering near-term products/enhancements to acquisition ▪ Customer IPT controlled ▪ Cost, schedule, capability metrics	▪ High-risk/High payoff ▪ "Game changer/Leap ahead" ▪ Prototype, Test and Deploy ▪ HSARPA
Basic Research (>8 yrs)	**Other (0-8+ years)**
▪ Enables future paradigm changes ▪ University fundamental research ▪ Gov't lab discovery and invention	▪ Test & Evaluation and Standards ▪ Laboratory Operations & Construction ▪ Management & Administration

DHS Science & Technology Investment Portfolio

Basic Research (> 8 years)

The S&T Directorate's basic research portfolio addresses long-term research and development needs in support of DHS mission areas that will provide the Nation with an enduring capability in homeland security. This type of focused, protracted research investment has the potential to lead to paradigm shifts in the Nation's homeland security capabilities.

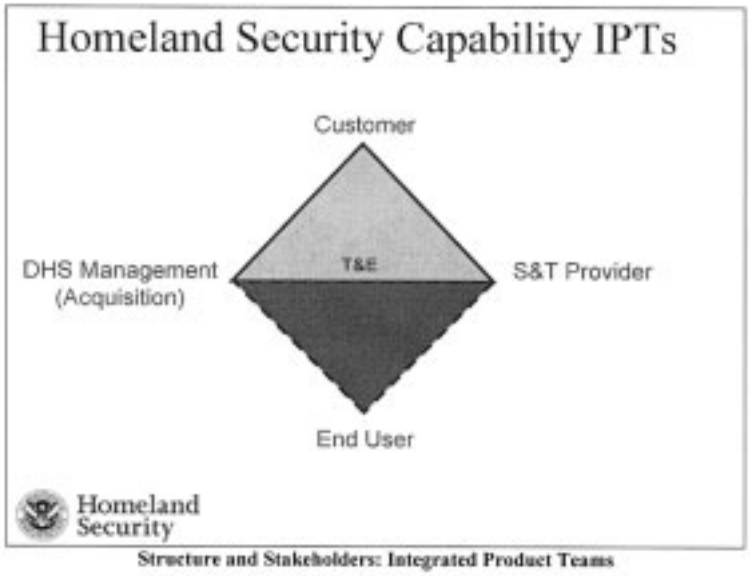
The S&T Directorate's basic research program enables fundamental research at our universities, government laboratories and in the private sector. Approximately $95 million is allocated for basic research in FY 2007 and $86 million or 13 percent of S&T's RDT&E budget, is allocated in FY 2008. Eventually, I would like up to 20 percent of the S&T Directorate budget allocated for basic research. It is critical that basic research be funded at consistent levels from year to year to ensure a continuity of effort from the research community in critical areas that will seed homeland security science and technology for the next generation of Americans and prevent technological surprise.

Product Transition (0 to 3 years)

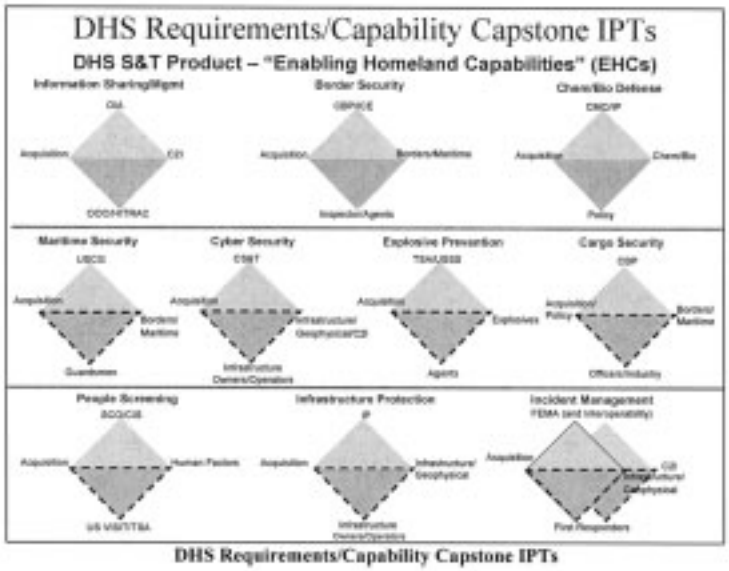
The centerpiece of the S&T Directorate's product transition portfolio are Capstone Integrated Product Teams (IPT) that function in mission-critical areas to identify our customers' needs and enable and transition near-term capabilities for addressing them. These Capstone IPTs engage DHS customers, acquisition partners, S&T technical division heads, and end-users as appropriate in our product research, development, transition and acquisition activities.

The IPT process enables our customers to identify and prioritize their operational capability gaps and requirements and make informed decisions about technology investments. The S&T Directorate, in turn, gathers the information it needs to respond with applicable technology solutions for closing these capability gaps. The science and technology solutions that are the outcome of this process, referred to as Enabling Homeland Capabilities, draw upon technologies that can be developed, matured, and delivered to our customer acquisition programs within three years.

Capstone IPTs have been established in 10 major areas: Information Sharing/Management; Cyber Security; People Screening; Border Security; Chemical/Biological Defense; Maritime Security; Explosive Prevention; Cargo Security; Infrastructure Protection; and Incident Management (includes first responder inter-operability).



Structure and Stakeholders: Integrated Product Teams



DHS Requirements/Capability Capstone IPTs

The S&T Directorate's product transition/IPT process ensures that appropriate technologies are engineered and integrated into the DHS acquisition system for our customers. The $343 million allocated for product transition for FY 2008 represents nearly half of my RDT&E budget.

The IPT process has created an excellent forum for the S&T Directorate to gain a better understanding of the most important issues of our customer agencies. Another tangible benefit of this Capstone IPT process has been improved coordination in addressing common functional challenges across the Department. This is due in large measure to the enthusiastic participation of DHS agency heads such as TSA Administrator Kip Hawley, Secret Service Director Mark Sullivan, and Border Patrol Chief David Aguilar and many other DHS leaders who have all personally chaired the IPTs relevant to their interests.

In FY 2008, the S&T Directorate plans to transition or transfer four programs that pre-date the IPT process. These programs have reached technical maturity and will be transferred to other DHS agencies who will be responsible for their continued operation. The budget request reflects the transfer to the Office of Health Affairs of the operations portions of BioWatch 1 & 2, the Biological Warning and Incident Characterization (BWIC) system, and the Rapidly Deployable Chemical Detection System, totaling $84.1 million. Moving the operations portions of BioWatch out of S&T allows us to focus on completing the development of BioWatch 3. BioWatch is a bio-aerosol monitoring system designed to provide cities the earliest possible detection of a biological attack. BWIC interprets warning signals from BioWatch and public health surveillance data using incident characterization tools (e.g., plume and epidemiological models) to quickly determine the potential impacts a release may have. Together, these two systems provide emergency personnel with the information they need to respond effectively and initiate life-saving medical countermeasures. In addition, the FY 2008 budget request reflects the transfer of the non-R&D component of the SAFECOM program to the National Protection and Programs Directorate, totaling $5.0 million.

It is important that the S&T Directorate also engage the emergency responder community and address operational issues to help them do their jobs more quickly, effectively and safely. S&T's Technology Clearinghouse and TechSolutions initiatives provide direct support to emergency responders' technology needs. The Technology Clearinghouse, created in accordance with a provision of the *Homeland Security Act of 2002,* is designed to be a "one-stop shop" for access to technology information for federal, State, and local public safety and first responder communities.

TechSolutions provides a Web-based mechanism for responders to register their input regarding capability gaps that need to be addressed to help them in their jobs. S&T responds by identifying existing technology that may meet the need, or if nothing is available, proceeding with the rapid prototyping of an appropriate solution to be fielded in less than 18 months. S&T also houses the Office for Inter-operability and Compatibility, which includes some components of the legacy SAFECOM program and aims to increase levels of emergency responder inter-operability by developing tools and methodologies, as well as advancing standards that emergency response agencies can put into effect.

Innovative Capabilities (2 to 5 years)

S&T's Innovation/HSARPA portfolio supports a key goal of mine for the Directorate in its efforts to put advanced capabilities into the hands of our customers as soon as possible. It has made important inroads in research areas aligned with our DHS customers. Toward this end, S&T has introduced two important new initiatives. One of these, Homeland Innovative Prototypical Solutions (HIPS) is designed to deliver prototype-level demonstrations of game-changing technologies within two to five years.

The second initiative, High Impact Technology Solutions (HITS), is designed to provide proof-of-concept solutions within one to three years that could result in high-payoff technology breakthroughs. While these projects are very high-risk, they offer the potential for "leap-ahead" gains in capability should they succeed. While projects are separately budgeted in "Innovation/HSARPA" (based on moderate to high risk with a high payoff, if successful), ALL are executed within the six technical divisions.

The S&T Directorate also continues to manage an active Small Business Innovative Research (SBIR) program on behalf of DHS that currently issues two solicitations each year and generates multiple awards for the small business community. The first solicitation for FY 2007 opens in mid-February and the second solicitation is planned for release in May. The solicitations will address topics in areas that are aligned with the six technical divisions.

The Innovation/HSARPA portfolio is receiving $60 million in FY 2008 funding for the innovative/leap-ahead HIPS and HITS projects. Because of the short timeline for HIPS and HITS, we anticipate that these projects will respond to the urgent needs of the DHS components for solutions to fill capability gaps.

ENABLING U.S. LEADERSHIP IN SCIENCE & TECHNOLOGY

University-Based Centers of Excellence

The S&T Directorate is developing a robust, results-oriented network of Homeland Security Centers of Excellence (COEs) to leverage the independent thinking and ground-breaking capabilities of the Nation's colleges and universities. The COEs are conducting multi-disciplinary research and education, each focused on an area critical to homeland security. The Office of University Programs is providing the communications and infrastructure to produce, share, and transition the Centers' research results, data, and technology to customers and end-users.

Currently, seven pre-existing COEs connect experts and researchers at more than 80 colleges and universities, including several Minority Serving Institutions (MSI). More than 20 partners representing industry, laboratories, think tanks, nonprofit organizations, and other agencies also participate. University Programs is coordinating COE efforts with other S&T Directorate-sponsored, university-based initiatives. Under the new S&T organizational construct, existing COEs are being strategically aligned with at least one S&T division, or to Directorate-wide activities such as Operations Analysis and the Homeland Security Institute, in a structure that will best support the Divisions' fundamental research and development activities and other requirements.

We are proceeding with plans to establish four additional COEs over the next two fiscal years to help round-out the Directorate's need for university-based fundamental research. The new COEs will combine the research missions of some existing COEs and add new research areas under the division-aligned construct to meet DHS needs. S&T has released Broad Agency Announcements (BAAs) regarding plans to establish new COEs in the areas of explosives detection, mitigation, and response; border security and immigration; maritime, island, and extreme/remote environment security; and natural disasters, coastal infrastructure and emergency management. The competitive selection process is designed to ensure that institutions of high quality and academic merit participate from as many areas of the United States as practicable.

DHS Scholars and Fellows Program

DHS education programs are helping to attract and nurture future scientific leaders for the homeland security workforce and to strengthen the expertise of our existing labor pool. University Programs is engaging high-performing students through the DHS Scholars and Fellows program. Increasingly, S&T's scholarships and fellowships will become aligned to the Centers of Excellence and to the DHS mission. During this period of transition, we will honor our commitments to all currently participating Scholars and Fellows.

The FY 2008 budget requests $38.7 million for S&T's University Programs, which includes the Homeland Security Centers of Excellence and the Scholars and Fellows Program.

Office of National Laboratories

In carrying out its mission, the S&T Directorate works to develop, sustain, and renew a coordinated network of DOE National Laboratories, federal laboratories and University Centers, the infrastructure needed by multi-disciplinary teams of scientists, engineers and academics to discover, develop and transition homeland security capabilities to operational end-users.

The FY 2008 budget request includes $88.8 million for the Office for National Laboratories (ONL), through which the S&T Directorate's laboratory facilities programs are executed. ONL provides the Nation with a coordinated, enduring core of productive science, technology and engineering laboratories, organizations and institutions, which can supply knowledge and technology required to secure our homeland. In addition to oversight of laboratory operations in direct support of the Department and its missions, ONL also has the specific responsibility for coordinating homeland security-related activities and laboratory-directed research conducted within the DOE National Laboratories.

Industry Participation in DHS Science & Technology

Industry is a valued partner of DHS S&T and its continued participation in developing solutions for homeland security applications is vital to our effort to safeguard the Nation. Consistent with S&T's new structure, our Innovation/HSARPA portfolio and six technical divisions will be releasing BAAs that seek industry participation to address specific challenges in their respective areas. For example, Innovation/HSARPA has already posted BAAs seeking expertise in tunnel detection technologies, container security (SAFECON program), and a mobile screening laboratory to support human screening R&D in the field.

Innovation/HSARPA plans to release six additional BAAs shortly to address areas that include critical infrastructure protection, hostile intent detection and other key areas. By spring 2007, we intend to issue a BAA for longer-term efforts that cover our complete innovation topic area portfolio.

No one knows where good ideas come from and for that reason I have been personally proactive in both seeking out and receiving technology briefs and opportunities. This is a culture I am working to instill throughout the DHS S&T Directorate.

The *Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act of 2002,* administered in the S&T Directorate, is proving to be a valuable tool in expanding the creation, proliferation and use of cutting edge anti-terrorism technologies throughout the United States. Over the past year we have made significant improvements in implementing the Act, including a new Rule; a revised, streamlined Application Kit; new coverage for emerging technologies that are undergoing test and evaluation; increased use of pre-application teleconferences between SAFETY Act technology evaluators and applicants to review requirements and answer questions prior to submitting a full application; and formal procedures to expedite applications for technologies involved with pending government procurements. The Office of SAFETY Act Implementation (OSAI) has made significant strides in reducing application processing time and providing more Qualified Anti-Terrorism Technologies (QATTs) that could save lives. Through increased efficiencies and process improvements, the average time to process SAFETY Act applications has been reduced from 233 days in the early days of the program to less than 140 days in FY 2007. As of February 2007, OASI has received 223 full applications and 376 pre-applications. A total of 137 SAFETY Act awards have been granted—87 applications have qualified for both Designation and Certification and 50 have received Designation only. I am mindful of the interest in this program in the Congress and across the Nation.

As part of our outreach efforts to encourage greater industry participation, the Directorate is hosting the first Homeland Security Science & Technology Stakeholders Conference, May 21–24. The conference will inform government, industry and aca-

demia of the direction, emphasis, and scope of the research investments by the S&T Directorate, and provide information about business opportunities. The conference will present the Directorate's new organization, explain how to do business with the DHS S&T research enterprise, and provide visibility into new and emerging technologies through an Innovation Gateway Marketplace. I hope you will join us for this event at the Ronald Reagan Building and International Trade Center.

FY 2008 BUDGET OVERVIEW

Science and Technology Directorate's budget request of $799.1 million includes $142.6 million for Management and Administration (M&A) and $656.5 million for research, development, testing and evaluation. M&A funds federal employees' salaries, benefits, travel, and other expenses at Headquarters and the S&T laboratories. This staff maintains oversight of S&T's extensive day-to-day technical and administrative operations. M&A also funds business operations, including working capital fund, and management support. Research, Development, Acquisition and Operations supports the needs of the operational components of the Department and is categorized to match the new S&T organization. The basic research, product transition and innovation R&D activities undertaken by S&T cut across the Directorate and its divisions and are incorporated into the following projects and programs that are included in the President's budget for FY 2008.

- The $25.9 million requested for *Borders and Maritime Security* will support technology development for the Secure Border Initiative (SBI), a comprehensive multi-year plan to secure America's borders. This Division is providing the tools, processes, and manpower to ensure SBI implementation is effective and affordable. We are working directly with the SBI program executive office to provide a transformation strategy for SBI; develop the next generation of modeling and analysis tools for strategic planning; and provide systems engineering support. The Division will also develop and transition technologies to industry to reduce risk and support border security programs like SBInet, a technology acquisition program under the Customs and Border Protection SBInet Program Management Office.

  We are also developing technologies to ensure the integrity of cargo shipments with known origins, and to better target suspicious shipments, and to enhance the end-to-end security of the supply chain—from the manufacturer of goods to final delivery. One of the most significant potential terrorist threats to the Nation is the vast numbers of shipping containers that flow through our borders each year, most of which enter without physical inspection. Technologies and processes developed within this area will assure government customs and shippers of the integrity of shipping containers and its cargo and communicate the container's status as well as security information. By employing a system-of-systems approach, this will deliver technological capabilities to DHS customers and end-users that address supply chain vulnerabilities. These capabilities are directed toward enhanced physical security and information management, and bound by a security architecture which encompasses the world's supply chain.
- The $228.9 million requested for *Chemical and Biological* will provide the basic knowledge, technologies and systems needed to protect against possible chemical and biological attacks on the Nation's population, agriculture or infrastructure. The greatest emphasis is on those biological attacks that have the greatest potential for widespread catastrophic damage to the population. These include—but are not limited to—aerosolized anthrax, and smallpox.

  The Division conducts material threat and risk assessments on both naturally occurring and engineered agents; conducts experiments to close major scientific knowledge gaps that could have a large impact on how the Nation responds to a biological attack; and provides scientific support to the intelligence community. As such, the primary output is an intelligence-informed, scientific characterization and prioritization of the bio-terrorist risks to be used by the Homeland Security Council and partnering agencies (e.g., Department of Health and Human Services, Environmental Protection Agency, Department of Agriculture, and the Intelligence Community).

  Based on this knowledge, we are developing effective measures for deterrence, detection, and mitigation of biological terrorism acts against the U.S. population, infrastructure, and agricultural system. This includes developing tools to meet federal, State, and, local emergency responder needs such as operational models to support Interagency Modeling and Atmospheric Assessment Center (IMAAC).

The Division is developing next-generation, biological-threat-agent detectors that recognize the signatures or fingerprints of biological agents. These detectors will be incorporated into the BioWatch system to substantially increase the system's capabilities and significantly reduce the response time. Other significant program activities include developing biological aerosol detection and sensor systems for monitoring the Nation's critical infrastructure such as government buildings, airports, subways, office buildings, shopping malls, sports arenas, hotels and hospitals. These "detect-to-protect" systems detect biological agents within minutes (acting as reliable 'smoke alarms') to protect high value facilities and their occupants. Many of the technologies being developed in this program will be manufactured and used by the private sector.

Chemical countermeasures work enhances the Nation's capability to anticipate, prevent, protect from, respond to and recover from chemical terrorist attacks. The chemical threat spectrum comprises a broad array of chemicals, to include chemical warfare agents, toxic industrial chemicals, and non-traditional agents (NTAs). Existing and emerging chemical warfare agents can potentially be used against virtually any civilian target resulting in significant loss of life and impedance in the use of key infrastructure. Chemical countermeasures addresses these threats by: enabling comprehensive understanding and analyses of chemical threats; developing pre-event assessment, discovery, and interdiction for chemical threats; developing warning, notification, and timely analysis of chemical attacks; optimizing technology and process for recovery from chemical attacks; and enhancing the capability to identify a chemical attack's source.

- The $63.6 million requested for *Command, Control and Inter-operability* will fund programs focused on cyber security; communications, compatibility and inter-operability; and knowledge management.

  Cyber security research, development, testing and evaluation is focused on improving the security of the existing cyber infrastructure and providing a foundation for a more secure infrastructure through coordinated efforts with other government agencies and private industry. Cyber attacks on U.S. information networks can have serious consequences such as disrupting critical operations, causing loss of revenue and intellectual property, or loss of life. The Division also addresses cyber security requirements from internal Department customers in support of the DHS's operational missions in critical infrastructure protection. It also addresses related aspects of national security and emergency preparedness telecommunications.

  Communications, inter-operability and compatibility programs within Command, Control and Inter-operability strengthen inter-operable wireless communications, improve effective information sharing, and develop tools to enhance overall coordination and planning at all levels of government. Currently, the Nation's capacity for inter-operable communications is hindered by sub-optimized planning and coordination, and the Office for Inter-operability and Compatibility is working to strengthen and integrate inter-operability and compatibility.

  We are also developing knowledge management tools to reduce the risk of terrorist attacks and to prepare for and respond to natural and man-made disasters. This will provide new capabilities for the DHS Intelligence & Analysis Directorate and the DHS information enterprise for the integration, management, analysis, and dissemination of actionable information. This knowledge management research provides tools and methods to handle massive amounts of information that is widely dispersed in a great variety of forms. Being able to find such information, understand its meaning, and then use it to assess an actual threat and determine the level of risk before an attack or incident occurs is the best way to save lives and preserve our way of life.

- The $63.7 million requested for *Explosives* will fund programs focused on the detection, mitigation, and response to explosives threats such as improvised explosive devices (IEDs) and suicide bombers. The Division employs a broad range of existing and emerging approaches to detect and lessen the impact of explosive materials. These include baggage-screening devices as well as the capability to identify explosives residue. Terrorist events like the Madrid rail bombing, the London Underground attack, and the recent disclosure of planned attacks on U.S.-bound flights from the United Kingdom, all involved explosive threats. Those events underscore the operational need for a unified

approach to the detection of, response to, and mitigation of explosive threats across all modes of transportation.

In explosives detection, we are improving existing explosive detection methods, developing new technologies, and integrating improvements and technological developments into both deployed and new systems. Detection is a key defense against successful attacks. For example, the Check Point Program applies to multiple venues where real or virtual portals exist. Historically, airports have received the most attention, but similar portal situations can be found at rail stations and cruise ship terminals. Check point programs address suicide bombers, carry-ons, leave-behind IEDs, and vehicle-borne IEDs. The two other principal programs in this area are checked baggage and cargo. Like aviation, rail and ship modes share checked baggage and cargo screening challenges.

The check point program addresses the risk of catastrophic loss of mass transit resulting from small IEDs detonated in passenger cabins and the catastrophic loss or hostile takeover of mass transit resulting from the presence of certain weapons in passenger cabins. The principal objective of the program is developing advanced technology for integration with future check point systems to detect explosives and concealed weapons, while meeting requirements for automation, efficiency, and cost reduction. Longer-term objectives include applying systems integration and a seamless flow of information with reduced impact to the checkpoint operations environment. The program also strives to upgrade currently deployed technologies to address emerging threats and concealment methods.

The checked baggage program identifies and develops the next generation of checked baggage screening systems, and supports continuous improvements toward the Congressionally directed goal of 100 percent screening of aviation checked baggage by electronic or other approved means with minimum or no impact to the flow of people or commerce. Checked baggage will focus on continuing work with Manhattan II by conducting system development and integration of the Manhattan II checked baggage program, complete the preliminary system architecture test and evaluation, and conduct detection-technology test and evaluation.

The cargo program is developing the next generation of air cargo screening systems, with transition targeted for FY 2011.

- The $12.6 million requested for *Human Factors* will apply the social and behavioral sciences to improve detection, analysis, and the understanding of threats posed by individuals, groups, and radical movements. This knowledge will support the preparedness, response and recovery of communities impacted by catastrophic events and to advance national security by integrating human factors into homeland security technologies. Further this will enhance the capability to control movement of individuals into and out of the United States and its critical assets through accurate, timely, and easy-to-use biometric identification and credentialing validation tools.
- The $24.0 million requested for *Infrastructure and Geophysical* will develop technical solutions and reach-back capabilities to improve State, local, tribal, and private sector preparedness for and response to all hazardous events impacting the population and critical infrastructure.

The Division's focus is on identifying and mitigating the vulnerabilities of the 17 critical infrastructure sectors and key assets that keep our society and economy functional. The Division models and simulates the Nation's critical infrastructures to determine how various scenarios will affect each sector, provides decision support tools to guide decision-makers in identifying gaps and vulnerabilities, and develops predictive tools and methods to aid in preparing for and responding to various catastrophes. Additionally, the Division focuses on responder preparedness and response capabilities that improve the ability of the Nation to prepare for, respond to, and recover from all-hazards emergencies. Applying the best available science and technology for the safety and security our emergency responders and homeland security professionals ensures they may effectively perform their jobs—saving lives and restoring critical services.

The Division is also developing a capability that will enable owners and operators of the most vital critical infrastructure sites to implement affordable and reliable blast and projectile mitigation measures improving capabilities

to withstand these threats. The program is developing suites of advanced materials, design procedures, and innovative construction methods that can be used to protect critical infrastructure and key resources.

In addition, the Division is developing decision-making and information-sharing tools to aid responders. This will dramatically enhance the information management and information sharing capabilities of incident commanders and emergency responders as emergencies increasingly demand more highly coordinated responses.

- The $59.9 million requested for *Innovation/HSARPA* will focus on homeland security research and development that poses a risk of failure, but if successful would lead to significant technology breakthroughs that would greatly enhance DHS operations. HSARPA carries out its activities in two areas: (1) Homeland Innovative Prototypical Solutions, which are designed to deliver prototype-level demonstrations of game-changing technologies in two to five years. These programs are moderate risk, but offer high pay-off and (2) High Impact Technology Solutions, which are designed to provide proof-of-concept answers that could result in high-payoff technology breakthroughs. Though there is a considerable risk of failure, these projects offer the potential for significant gains resulting from success.
- The $88.8 million requested for *Laboratory Facilities* will fund operation of the S&T laboratory facilities, including Plum Island, the Transportation Security Lab, Environmental Measurements Laboratory, the Chemical Security Analysis Center, and the National Biodefense Analysis and Countermeasures Center. Laboratory Facilities also funds design work on the National Bio and Agrodefense Facility and upgrade of the Plum Island facility.
- The $25.5 million requested for *Test & Evaluation and Standards* funds two areas Test and Evaluation (T&E) and Standards. T&E works across DHS and ensures that systems meet the capability needs of users, validates performance and provides measurable improvement to operational capabilities. Effective testing and evaluation programs provide crucial information to decision-makers for acquisition and deployment of technology. Standards are consensus based measures—from basic specifications to performance criteria—that give DHS and its customers confidence that technology and systems will perform as required. The S&T Directorate works across DHS and with numerous external partners to build consensus and support development of needed standards.
- The $24.7 million requested for *Transition* programs will expedite technology transition to deliver near-term products and technologies to meet DHS component requirements. This area also funds the Office of the SAFETY Act Implementation, transition support programs such as the Technology Clearinghouse, and the S&T Directorate's international and interagency programs.
- The $38.7 million requested for *University Programs* will allow the S&T Directorate to engage the academic community to support current DHS priorities and enhance homeland security capabilities by providing ground-breaking research, analyses and educational approaches. The program is designed to bring together the best scientific talent and resources from U.S. academic institutions to help solve complex and technologically challenging homeland security problems facing our nation. Program activities simultaneously focus on building homeland security expertise in the academic community, creating strategic partnerships, and fostering a new generation of homeland security experts.

  The program works to:

  - Strengthen U.S. scientific leadership in homeland security research;
  - Generate and disseminate knowledge and technical advances to aid homeland security frontline professionals;
  - Foster a homeland security culture within the academic community through research and education programs; and
  - Build a highly-trained science and engineering workforce dedicated to homeland security that will sustain progress over time.

  This program invests in two areas: the university-based Centers of Excellence, and student Scholarships and Fellowships intended to build and develop the next generation of academic researchers in disciplines that are relevant and essential to homeland security.

Department of Homeland Security
Science and Technology Directorate
Research, Development, Acquisitions, and Operations
Summary of FY 2008 Budget Estimates by Program/Project Activity
(Dollars in Thousands)

NEW RESEARCH, DEVELOPMENT, ACQUISITION, AND OPERATIONS BUDGET STRUCTURE

Program/Project Activity	FY 2006 Actual		FY 2007 Revised Enacted 1/		FY 2008 Request		Increase (+) or Decrease (-) For FY 2008					
							Total Changes		Program Changes		Adjustments-to-Base	
	FTE	AMOUNT	FTE	AMOUNT	FTE	AMOUNT	FTE	AMOUNT	FTE	AMOUNT	FTE	AMOUNT
Borders and Maritime Security		$72,607		$33,436		$25,936		($7,500)		(7,500)	---	$0
Chemical and Biological 2/		$490,319		$313,553		$228,949	---	(84,604)			---	(84,604)
Command, Control, and Interoperability 3/		$108,550		$62,612		$63,600	---	988			---	988
Explosives		$83,094		$105,231		$63,749	---	(41,482)		(41,482)	---	---
Human Factors		$6,924		$6,800		$12,600	---	5,800		5,800	---	---
Infrastructure and Geophysical		$47,186		$74,781		$24,000	---	(50,781)		(50,781)	---	---
Innovation		$0		$38,000		$59,900	---	21,900		21,900	---	---
Laboratory Facilities		$96,987		$105,649		$88,814	---	(16,835)		(16,835)	---	---
Test and Evaulation , Standards		$32,399		$25,432		$25,520	---	88			---	88
Transition		$6,814		$24,040		$24,700	---	660			---	660
University Programs		$43,622		$48,575		$38,700	---	(9,875)		(9,875)	---	---
Subtotal, Enacted Appropriations and Budget Estimates	---	**$988,502**	---	**$838,109**	---	**$656,468**	---	**($181,641)**	---	**($98,773)**	---	**($82,868)**
Less: Adjustments for Other Funding Sources:												
Less Prior Year Recission, P.L. 109-295		($20,000)		($125,000)								
Net, Enacted Appropriations and Budget Estimates	---	**$968,502**	---	**$713,109**	---	**$656,468**	---	**($181,641)**	---	**($98,773)**	---	**($82,868)**

1/ FY 2007 funding is represented as "revised enacted" due to the realignment of the budget to reflect the organizational changes in FY 2007.
2/ Reflects ($84,100) transfer to OHA
3/ Reflects ($5,000) transfer to NPPD

CONCLUSION

In conclusion, I am pleased to report that the S&T Directorate is well positioned today to mobilize the Nation's vast technical and scientific capabilities to enable solutions to detect, protect against and recover from catastrophic events.

Our plans for restructuring the organization have been implemented and it is indeed gratifying to see that they appear to be working as we advance to the critical phase of product transition. Increasingly, our DHS customers are recognizing the substantial value that S&T's technical expertise brings to their operations. We have engaged them, eliciting participation at the highest levels, to join us at the table to work constructively on solutions for countering the formidable threats this nation faces.

We appreciate the many demands on the taxpayers' precious dollars and you have my commitment that the S&T Directorate will be wise stewards of the public monies you have entrusted to us. We are steadfast in our resolve to serve the best interests of the Nation by investing in the talent and technology that will provide America with a sustainable capability to protect against acts of terror and other high-consequence events for generations to come.

Members of the Committee, I thank you for the opportunity to meet with you today to discuss a newly realigned Science & Technology Directorate that is meeting homeland security challenges with a renewed sense of purpose and mission. I look forward to working with you throughout the 110th Congress.

BIOGRAPHY FOR JAY M. COHEN

Department of Homeland Security, Under Secretary for Science and Technology, Jay M. Cohen is a native of New York. He was commissioned in 1968 as an Ensign upon graduation from the United States Naval Academy. He holds a joint Ocean Engineering degree from Massachusetts Institute of Technology and Woods Hole Oceanographic Institution and Master of Science in Marine Engineering and Naval Architecture from MIT.

His early Navy assignments included service on conventional and nuclear submarines. From 1985 to 1988 Cohen commanded USS HYMAN G. RICKOVER (SSN 709).

Following command, he served on the U.S. Atlantic Fleet as a senior member of the Nuclear Propulsion Examining Board, responsible for certifying the safe operation of nuclear powered ships and crews.

From 1991 to 1993, he commanded USS L.Y. SPEAR (AS 36) including a deployment to the Persian Gulf in support of Operation DESERT STORM.

After Spear, he reported to the Secretary of the Navy as Deputy Chief of Navy Legislative Affairs. During this assignment, Cohen was responsible for supervising all Navy-Congressional liaison.

Cohen was promoted to the rank of Rear Admiral in October 1997 and reported to the Joint Staff as Deputy Director for Operations responsible to the President and DOD leaders for strategic weapons release authority.

In June 1999, he assumed duties as Director Navy Y2K Project Office responsible for transitioning all Navy computer systems into the new century.

In June 2000, Cohen was promoted in rank and became the 20th Chief of Naval Research. He served during war as the Department of the Navy Chief Technology Officer (a direct report to the Secretary of the Navy, Chief of Naval Operations and Commandant of the Marine Corps). Responsible for the Navy and Marine Corps Science and Technology (S&T) Program (involving basic research to applied technology portfolios and contracting), Cohen coordinated investments with other U.S. and international S&T providers to rapidly meet war fighter combat needs. After an unprecedented five and a half year assignment as Chief of Naval Research, Rear Admiral Cohen retired on February 1, 2006.

Under Secretary Cohen was sworn in to his current position at the Department of Homeland Security on August 10, 2006.

Chairman WU. Thank you, Mr. Under Secretary. Director Oxford.

STATEMENT OF MR. VAYL S. OXFORD, DIRECTOR, DOMESTIC NUCLEAR DETECTION OFFICE, DEPARTMENT OF HOMELAND SECURITY

Mr. OXFORD. Good morning, Chairman Wu, Ranking Member Gingrey, and other Members of the panel. I would like to thank the

Committee for the opportunity to present DNDO's research and development priorities for fiscal year 2008. I am pleased to be here with my colleague, Under Secretary Cohen, and other colleagues from past lives that are with me also here on the panel.

DNDO is chartered to develop a global nuclear detection architecture that would form a robust defensive layer to prevent nuclear and radiological terrorism. We are also asked to direct all radiation detection development programs on behalf of DHS and to work as the U.S. Government collaborator with other Departments regarding research and development for the radiological and nuclear area.

We invest in the enhancement of existing technologies through both a near-term spiral development program, as well as a transformational research and development program to deliver revolutionary improvements in the performance of nuclear detection systems. Today I will highlight the near-term and transformational plans for 2008, and touch upon how DNDO coordinates its R&D activities with other federal agencies.

Regarding near-term R&D priorities, we feel we must finish the work of securing our nation's ports of entries. However, we cannot ignore the possibility that a terrorist might attempt to illicitly transport a nuclear or radioactive material between the ports of entry.

DNDO's near-term focus is on making further improvements to radiation detection capabilities for the national ports of entry, while also developing solutions for non-ports of entry threats. We are testing the Advanced Spectroscopic Portal at the Nevada Test Site and the New York Container Terminal. Results of these tests will be used to support the Secretary's certification decision as required by the 2007 Appropriations Bill. And in 2008, we will also complete development and begin production for ASP variants to include mobile truck mounted systems, as well as shuttle carrier systems that address specific challenges presented at some of our sea ports that load cargo directly from ships to rail. The Cargo Advanced Automated Radiography System will automatically detect high density shielding within cargo that could escape the detection by our passive systems. The automated imaging processing capabilities and vision for CAARS will substantially improve throughput rates over current generation radiography systems.

Development of these technologies will continue in 2008, with prototypes being delivered in mid 2009. DNDO's Human Portable Radiation Detection System Program will improve current and backpack radiation detection systems by improving identification capabilities, standardizing displays and controls, reducing weight, and improving system connectivity so that data can be rapidly communicated and analyzed.

Within our long-term transformational research program we include an exploratory research program, a dedicated Academic Research Initiative, and several upcoming advanced technology demonstrations. In exploratory research we have initiated 44 projects with our national laboratories. We have recently awarded seven cooperative agreements with academia, and next week we will announce 10 awards with private industry. These efforts have already begun to pay off.

An automated process established at Lawrence Berkeley National Laboratories allows us to evaluate over 100 new detector materials per month or over 1,000 per year, a tenfold increase over previous capabilities within this country. Proof of concept efforts on several standoff technologies have demonstrated that very small amounts of material can be detected at 20 miles per hour from a distance of over 65 meters. Again, a tremendous improvement over previous and current capabilities.

In 2008, our Advanced Technology Demonstration Programs will include an Intelligent Personal Radiation Locator that responds to a user requirement to improve upon capabilities in personal radiation devices for discrimination as well as localization of threat materials. Our Standoff Detection Advanced Technology Demonstration will develop and evaluate technologies to significantly increase detection ranges out to 100 meters. The verification of Shielded Special Nuclear Material Advanced Technology Demonstration will develop and test advanced technologies to verify the presence of special nuclear material in cluttered environments and may lead to a human portable capability to automatically verify the presence of shielded special nuclear material.

Finally, a survey by the National Science Foundation and the Department of Energy showed a downward trend in this nation's nuclear science expertise. In 1980, there were 65 nuclear engineering departments in our U.S. universities. Today there are 29. Currently it is estimated that one-third to three-quarters of the current nuclear workforce will reach retirement age in the next 10 years. DNDO's Academic Research Initiative will spur the academic community to provide the nuclear detection experts of the future by funding universities to conduct R&D in the areas relevant to nuclear detection. Last month DNDO and the National Science Foundation solicited grant applications from our colleges and universities to help begin this new academic initiative.

Regarding coordination with other organizations, we recognize that several federal agencies already engage in research in this area, so we have coordinated our activities with the National Nuclear Security Administration, the Defense Threat Reduction Agency, and the Director for National Intelligence. Several mechanisms are currently in place to insure active coordination of these efforts. These include joint participation in the Domestic Nuclear Research and Development Working Group, chaired by the President's science advisor, an interagency working group that is intended to create an R&D roadmap for the future.

DNDO also supports Department of Energy activities by jointly reviewing proposals that come into both organizations to make sure that we are collaborating and reducing the conflict of funding. We do that also with the Department of Defense.

Finally, in conclusion, let me say the challenges that lie ahead require coordinated effort on behalf of the best scientific minds in this country, from fostering the development of revolutionary detection technologies that fill gaps in our evolving architecture, to providing next-generation technologies that improve performance, cost, and operational value. DNDO is working to provide the Nation with a continuously improving capability to protect against a terrorist nuclear attack.

And I would at this time yield the rest of my time and be glad to answer any questions, Mr. Chairman.

[The prepared statement of Mr. Oxford follows:]

PREPARED STATEMENT OF VAYL S. OXFORD

Introduction

Good morning Chairman Wu, Ranking Member Gingrey, and distinguished Members of the Subcommittee. As Director of the Domestic Nuclear Detection Office (DNDO), I would like to thank the Committee for the opportunity to discuss our research and development (R&D) priorities for Fiscal Year 2008 and how these activities will directly enhance the probability of mission success. I am pleased to be here with other distinguished witnesses, Under Secretary Cohen, Mr. Czerwinski, Dr. Epstein, and Ms. Ward.

Key to the success of the Department of Homeland Security (DHS) is improving the Department's ability to mitigate risks across the entire threat spectrum. In recognition of the catastrophic risk posed by the use of a nuclear weapon within the United States, all nuclear detection research, development, test, evaluation, and operational support within the Department was consolidated into the DNDO in April of 2005. Since then DNDO has developed, and continues to evolve, the global nuclear detection architecture, while improving the domestic means to detect and report attempts to import or transport a nuclear device or fissile or radiological material intended for illicit use.

DNDO maintains a preeminent research and development program and capitalizes on the benefits of integrating this program with larger acquisition efforts. Over half of DNDO's Fiscal Year 2008 budget request is intended for R&D activities. We categorize our R&D work into two areas: enhancement of existing technologies through near-term, spiral development; and long-term transformational R&D that will deliver revolutionary improvements in the cost, performance and associated operational burdens of nuclear detection systems.

Today, I will be discussing both our near-term and transformational R&D plans for FY 2008. As I describe these efforts, I will share with you how DNDO uses architectural analysis and end-user requirements to help guide not only acquisition efforts, but also our research agenda. I will also touch upon how DNDO coordinates its scientific research and technical development activities with other federal agencies.

Near-Term R&D Priorities

Our analysis of the detection architecture concluded that we must finish the work of securing our nation's ports of entry (POEs). However, we cannot ignore the possibility that a terrorist might attempt to illicitly transport a nuclear device or radioactive material between the POEs. DNDO's near-term focus is on making further improvements to radiation detection capabilities for the Nation's POEs as well as developing solutions for non-POE applications. These include general aviation, small maritime craft, non-POE land border crossings, and State and local operations.

DNDO will continue our Advanced Spectroscopic Portal (ASP) program, which improves upon existing polyvinyl toluene (PVT)-based radiation portal monitors that are currently deployed at the Nation's POEs, and select foreign POEs through the DOE Megaports Initiative. ASP systems not only detect the presence of radiation, but also identify the radiation source, enabling the system to discriminate real threat alarms from alarms due to normally occurring radioactive material (NORM). Alarms due to NORM are also known as nuisance alarms. The use of spectroscopic identification dramatically reduces nuisance alarms, and will allow for considerably improved throughput at high-volume ports, while simultaneously improving security. DNDO awarded contracts to Raytheon Company, Thermo Electron Corporation, and Canberra Industries, Inc. for the development and production of ASP last July. Approximately $44.5 million was immediately provided to the three vendors. Based on results of system performance tests now underway and upon certification by the Secretary, DNDO plans to award up to $1.1 billion over a five-year period to complete ASP development and acquisition.

In FY 2008, we will complete development and test phases and begin production for: truck-mounted ASP systems that provide mobility for several applications, including relocatable chokepoint applications in State and local operations, or at low-volume POEs where fixed systems may not be cost effective; and shuttle carrier-mounted ASP systems that address the challenge presented by several seaports that load cargo directly from ships to rail cars, therefore bypassing typical exit gate screening operations. By developing additional passive detection design variants

that meet unique port requirements, DNDO will be well on its way to achieving technical solutions that enable us to screen 100 percent of cargo containers entering the United States. To support all of our passive systems, we will be upgrading the standard ASP cargo portals with software improvements and better controls and displays based on feedback that we receive from operational deployments.

The Cargo Advanced Automated Radiography System (CAARS) will automatically detect high-density material shielded within cargo that could escape detection by passive radiation systems, like ASP. The automated image processing techniques envisioned for CAARS will also substantially improve throughput rates over current-generation radiography systems. DNDO awarded contracts to L–3 Communications, American Science and Engineering, Incorporated, and SAIC for the development of CAARS last September.

Development of these technologies will continue in FY 2008, with a projected delivery of prototype units in mid-2009. Once ready, these systems will be subjected to a rigorous test program to evaluate the technology and to enter into engineering development. Test results will serve as a major factor in evaluating the performance of the three contractors and continuing with the next phase of the program, in which low-rate initial production will begin. DNDO will also begin preparations for pilot deployments to evaluate operational factors and conduct other deployment planning efforts such as site surveys and environmental impact assessments.

Nevertheless, ASP and CAARS deployed at our official POEs are not the only technologies needed to fulfill our nuclear detection architecture. The DNDO is also working on Human Portable Radiation Detection Systems, or HPRDS, that aim to improve on current hand-held and backpack radiation detection systems similar to those currently used by Customs Border and Protection (CBP) and the Coast Guard. These systems currently weigh ten to 25 pounds, and are generally operated as a secondary screening tool. When an alarm is detected, hand-held systems can then be used to isolate and identify the source of the radiation. The HPRDS program seeks to reduce the weight of systems to approximately five pounds, while simultaneously improving detection probabilities to as high as 90 percent when used in tertiary or confirmatory inspection applications; and also improve connectivity for alarm reporting and technical support. In October, five companies received awards—Smiths Detection, SAIC, Ortec, Sanmina-SCI, and Target Instruments.

In FY 2008, development efforts for the next generation of hand-helds and backpacks will focus on: improving the identification capabilities of human portable systems so they can distinguish between threat and non-threat material quicker and with greater accuracy; standardizing the displays and control functions to improve system operability for field operators; reducing the weight of units so they are less burdensome to use; and improving systems connectivity so that data can be rapidly communicated and analyzed to determine if it represents a potential threat.

Long-Term Transformational R&D Priorities

Despite the progression of our near-term R&D efforts, there are still key, long-term challenges and vulnerabilities in our detection architecture that require long-range, higher-risk research programs to deliver the highest payoff improvements in detection capabilities. One of the primary motives for the establishment of the DNDO was to create a mechanism for significant and sustained funding into radiation detection technologies through innovative approaches. Our transformational R&D program works with all sectors—National Laboratories, academia, and private industry—to seek dramatic technical improvements.

This is not research for the sake of research. This is a deliberate, focused effort to address significant capability gaps in our present detection architecture—gaps that cannot be filled with current technologies because of performance issues, cost, or lack of capability. Revolutionary advances in radiation detection technology could potentially impact all capability gaps in our present detection architecture, from a distributed network of inexpensive radiation detectors to highly sensitive, standoff detection systems for sensing mobile threats at speed. Many of these technical breakthroughs would directly address some of the opportunities and challenges I mentioned before, such as general aviation, small maritime craft, non-POE land border crossings, and State and local operations.

Our transformational research includes a robust Exploratory Research Program, a dedicated Academic Research Initiative, and several upcoming Advanced Technology Demonstrations (ATDs). Exploratory Research focuses on technical solutions that are at the feasibility phase and show significant promise, but require further concept development and demonstration. As solutions and concepts mature, technologies will transition either into enabling components for existing ATDs or will generate new ATD initiatives. The purpose of an ATD is to develop and test a device and generate the data needed to perform a preliminary cost-benefit analysis for a

technology. Successful research originating from our Academic Research Initiative will also transition to exploratory research or an ATD initiative.

In December 2005, DNDO published a Call for Proposals to the National Laboratories soliciting novel detection approaches, materials, and advanced technologies as part of our Exploratory Research program. DNDO received more than 150 proposals, and ultimately selected 44 for award, resulting in nearly $40 million in research programs. Similarly, DNDO released a solicitation for private industry and academia proposals in the same research topics. More than 200 white papers were submitted, and last month we announced the award of seven cooperative agreements with academia totaling approximately $3.1 million. The research topics of these universities include advances in materials, associated electronics, detection techniques, and enabling technologies to investigate and understand important and related phenomenology.

In FY 2008, exploratory research topics will include: new materials that have high energy resolution, high efficiency, and low cost; shielded special nuclear material (SNM) verification efforts that would enable highly penetrating, efficient, low-dose interrogation systems to address screening of general aviation, small boats, and occupied vehicles; new solutions for passive detection of SNM in general aviation, commercial air cargo, and boats and small ships near the U.S. coastline; and technology and concepts that offer significantly enhanced threat sensitivity with remote and distributed emplaced sensor networks. In addition, we will be working with the DHS Science and Technology Directorate to examine techniques for integrating explosives detection with radiological and nuclear detection, achieving single-device solutions.

Our ATD program takes leading edge technological concepts (in many cases technology demonstrated conceptually under Exploratory Research) and develops a performance test unit to conduct a realistic demonstration of capabilities. The results of the tests form the basis for a preliminary cost benefit analysis that is used to objectively determine whether the technology should transition to our Systems Development and Acquisition program.

In FY 2008, the Intelligence Personal Radiation Locator (IPRL) ATD that started in 2006 will result in a performance test unit that will be ready for testing. The IPRL emerged from an end-user requirement for a next-generation personal radiation detection system similar to the radiation pagers often used by CBP, first responders, and law enforcement officials. IPRL will have sufficient energy resolution and sensitivity to reliably discriminate between NORM, background, and potential threats, and will be used by law enforcement, first responder, counterterrorism, the intelligence community and others in routine activities and surveillance. DNDO awarded contracts worth up to $22M for the IPRL program last September. This enabled us to conduct the design and development work required to take IPRL from the conceptual phase and become ready for testing of IPRL performance test units in early FY 2009.

In addition, our Standoff Detection ATD will be ready for final system design review, with a mid-FY 2009 target for testing of the performance test units. This ATD will allow DNDO to develop and evaluate key existing technologies such as coded aperture and Compton imaging that may dramatically improve sensitivity and directional accuracy. Our goal is to extend nuclear detection ranges to as much as 100 meters, potentially providing the capability to locate and identify nuclear threat materials at greater distances for use in ground-based, airborne, and maritime platforms. Defense Threat Reduction Agency (DTRA) and the Department of Defense (DOD) also have strong requirements for long standoff capability for detection of nuclear materials. To de-conflict our programs, DTRA cites the need for very long standoff detection of one kilometer (1000 meters) or more. Since in most cases the goal of 100 meters is unattainable with current technologies, DTRA's current efforts are closely related to those of DNDO. Achieving our shared goal to improve capability for longer standoff detection will require the resources of both DHS and DOD.

Our Verification of Shielded SNM ATD is scheduled for preliminary design reviews in early FY 2009, with final system design review expected in late FY 2009. This ATD will develop and test advanced technology to resolve alarms and definitively verify the presence of SNM despite cluttered environments or intentional countermeasures like shielding. Furthermore, another embodiment of this technology may lead to a whole new capability for portable interrogation systems that will enable relocatable or human portable detection systems that can automatically verify the presence of shielded SNM.

The final component of our transformational R&D program provides a much needed emphasis in nuclear detection sciences, a field that has been in decline at American universities for years. A survey by the National Science Foundation showed a downward trend since the mid-1990s of nuclear scientists and engineers of approxi-

mately 60 per year. In 1980, there were 65 nuclear engineering departments actively operating in the U.S. universities; now there are only 29. Currently, it is estimated that one-third to three-quarters of the current nuclear workforce will reach retirement in the next 10 years. The future security of our nation requires such a rejuvenation effort at our universities. The current projections forecast a need for approximately 100 new Ph.D.s per year.

DNDO's Academic Research Initiative will spur the academic community to provide the nuclear detection experts of the future by funding universities to conduct R&D in areas relevant to the detection of nuclear and radiological material. In addition, the program will foster potentially high-risk but high-payoff ideas that could lead to solutions that have not yet been considered. Last month, DNDO and the National Science Foundation announced grant opportunities worth up to $58 million over the next five years for colleges and universities. Once this program matures, our estimate is that this initiative will produce 20 to 30 new Ph.D.s per year, while also addressing critical research needs. This will not address the need completely. But our efforts, combined with the academic support efforts of other federal agencies like the Department of Energy, will help provide the nuclear scientists and engineers of the future.

Coordination of Effort

The identification of gaps in nuclear detection capabilities justifies the need for a well-supported DNDO research and development program. At the same time, we recognize that several federal agencies already engage in research and development in this area. Therefore, the planning process for the DNDO transformational research agenda was coordinated with partners, including the DOE National Nuclear Security Administration's Nonproliferation and Verification Research and Development Program (NA–22), the Defense Threat Reduction Agency (DTRA), and the Office of the Director of National Intelligence (DNI). I would like to take a moment to describe several mechanisms currently in place to ensure active coordination between DNDO and other agencies funding related research and development.

From its founding, DNDO supported the Domestic Nuclear Defense Research and Development (DND R&D) Roadmap Working Group to develop a coordinated, interagency R&D roadmap that would enhance the breadth of domestic nuclear defense efforts to ensure a secure nation. The DND R&D Working Group was chartered by the Homeland Security Council/National Security Council Domestic Nuclear Defense (DND) Policy Coordinating Committee. The DND R&D Roadmap Working Group developed a long-term vision for domestic nuclear defense R&D. The scope of this working group covered the interagency coordination of: R&D strategies for domestic nuclear defense; the identification and filling of critical technology gaps; enhancing efforts to develop and sustain critical capabilities through appropriate investments in the foundational science and research; interagency funding for necessary science and technology; and collaboration and exchange of vital R&D information. DNDO co-chairs the working group on interdiction research and development.

DNDO has also supported the National Nuclear Security Administration in reviewing foundational science proposals for advanced detectors and materials. Staff from both NA–22 and DNDO served on each others' proposal review panels, in part to ensure that duplication of funding is minimized. This interaction helped ensure that DNDO transformational R&D programs are well coordinated with those of NA–22 (which focused on foundational science for advanced detectors and materials), enabling the U.S. Government to best utilize the expertise of the National Labs. DNDO conducted similar proposal reviews with DTRA.

DNDO, as an interagency office, has full-time detailees from agencies such as DOE and DOD. These individuals have provided invaluable expertise in all aspects of the DNDO mission. Our detailees enable us to maintain an open and productive dialogue with our interagency partners so that we can avoid duplication of effort and make strides toward the complete implementation of the proposed architecture.

Conclusion

The challenges that lie ahead require a coordinated effort on the behalf of the best scientific minds within our government, academia and the private sector. The DNDO has taken an end-to-end approach to research and development, systems development, and product improvement. From fostering the development of revolutionary detection technologies that fill gaps in our evolving architecture to providing next-generation technologies that improve performance, cost, and operational value, DNDO is working to provide the Nation with a continuously improving capability to protect against a terrorist nuclear attack.

This concludes my prepared statement. With the Committee's permission, I request my formal statement be submitted for the record. Chairman Wu, Ranking

Member Gingrey, and Members of the Subcommittee, I thank you for your attention and will be happy to answer any questions that you may have.

BIOGRAPHY FOR VAYL S. OXFORD

Mr. Vayl Oxford was appointed Director of the Domestic Nuclear Detection Office (DNDO) in September 2005, reporting to the Secretary of the Department of Homeland Security with responsibility for the establishment of the new, jointly staffed office and for directing all activities associated with the organization.

Prior to his appointment to DHS, Mr. Oxford served as the Director for Counter-proliferation (CP) at the National Security Council.

Before his assignment to the White House, Mr. Oxford was the Deputy Director for Technology Development at the Defense Threat Reduction Agency (DTRA).

From 1993 to 1998, Mr. Oxford served at the Defense Nuclear Agency, and, then, the Defense Special Weapons Agency as the Director for Counter-proliferation.

During his Air force tenure, Mr. Oxford held several positions associated with aircraft and weapons development, and war plans analysis in Europe and the Pacific. He also served as an Assistant Professor of Aeronautics at the United States Air Force Academy from 1982 to 1986.

Mr. Oxford is a graduate of the United States Military Academy and the Air Force Institute of Technology and the recipient of numerous military awards. He received the DOD ACTD Technical Manager of the Year Award in 1997. He was appointed to the Senior Executive Service in 1997 and received the Meritorious Executive Presidential Rank Award in 2002.

Chairman WU. Thank you, Director Oxford. Dr. Epstein.

STATEMENT OF DR. GERALD L. EPSTEIN, SENIOR FELLOW FOR SCIENCE AND SECURITY, HOMELAND SECURITY PROGRAM, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

Dr. EPSTEIN. Thank you, Mr. Chairman, Ranking Member Gingrey, and Members of the Subcommittee. Thank you for the opportunity to speak with you this morning.

Before I start, I can't help but point out that I first started studying the issues I am going to be talking with you about this morning working for this institution in an agency that unfortunately no longer exists. I used to be with the Congressional Office of Technology Assessment and wrote a report on the same things we have been talking about. And as much as I welcome the opportunity to speak with you today, frankly, you deserve better than that. You deserve better than one hearing with individual witnesses. You need your own folks, a dedicated office working on precisely the interface of technology and policy, not just for this committee but for practically every other committee on the Hill. So let me just command that I think that is a capability that could be used here on the Hill.

Let me get back to what you asked me to talk about. I would like to start off by highlighting just one or two factors I think we need to keep in mind when we address Homeland Security Science and Technology, make a few observations along with way about the fiscal year 2008 request from the Department, and then end up with one specific point on what has turned out to be a popular issue, that of Science and Technology education.

Let me start with I think the greatest challenge we face in managing an R&D portfolio for the Department of Homeland Security, which is looking over the entire menu of risks that are in front of us and deciding what it is we actually need to spend our money on. This forces us to compare some very different threats; nuclear

threats, biological threats, infrastructure, explosives, borders, cyber attacks, and all this fortunately in the absence of much of the data you would really want to do a quantitative risk assessment. These attacks have not happened much to date. We would like to keep it that way. But I think we need better tools, better analytical procedures, better processes to figure out how we actually make some of these high-level tradeoffs.

Before we say, before I spend a lot of money on this capability, which I might know how to do, what else might I be able to spend it on, and what more security could we get for that? I don't think there is going to be a magic spreadsheet that is going to come up with the right allocation among different priorities, but I do think we can have systems that are going to help make our decisions a little more transparent and highlight where it is that our gut hunches, our subjective probabilities really are making a big difference.

I would also like to talk about the time horizon of S&T research in the Department of Homeland Security. When the Department was first formed, the government had just realized it had this mission. There was not a long-standing base of work precisely on homeland security type issues. There were a lot of immediate needs, a lot of immediate capabilities that could fill those needs, and the decision made at the time to go for what I think has been called the low-hanging fruit, near-term research, but to defer the more basic and the longer-term investigations. That is an understandable decision at the time, but it is not sustainable. And I am pleased to see looking through this year's budget request that we have a more balanced portfolio of research and development, not just near-term programs but also longer-term programs, and I am particularly pleased to see that we are willing to take some risks. And that is essential.

A serious pathology that a technology development organization can run into, especially one that has to look at emerging technological threats, is to aim too low. Under Secretary Cohen is going to need your help in making sure he is not running into this problem, making sure his vision is far enough. The way you will know he is doing his job is if he can come back to you and report that he has failed. If he hasn't started some programs that just don't pan out, he is not being aggressive enough, and I think he can use your help in holding him to that.

And I would just now like to conclude on a note about the Homeland Security Science and Technology Fellows Program. This is an important program. I am pleased that the Department recognizes the importance of a strong national Science and Technology base, not just for the many other objectives that we draw on S&T for but particularly for the Department of Homeland Security mission. And the Department recognizes this responsibility to replenishing the supply of human resources in this arena. But I think the program actually could probably be modified so that the fellows not only contribute in general to the U.S. science and technology base but contribute specifically to Homeland Security missions. And this is not by making more requirements on the program but actually getting them more excited about homeland security and the technology applications that they can work on that are solving our own

needs. I think a deeper engagement with these fellows, they now have an orientation at the beginning of the process and they work on an internship, I think a continuing involvement, high-level mentorships, briefing them on threats facing the Nation and the different ways in which the whole Homeland Security architecture can address it will get them excited, not only about their own science and technology investigations, but about applying that to the homeland security mission.

And, again, we need S&T workforce in this country, but the homeland security agencies have a harder job. They have got to work with the U.S. citizens. We are fortunate to have foreign nationals contribute to the technical workforce in this country, but they can't get security clearances, and they can't work for the gentleman on my right. So the programs they are supporting are very important, and I think they can have a higher payoff in having them work directly for the Homeland Security sector.

So I would be glad to entertain your questions at the end of the panel.

[The prepared statement of Dr. Epstein follows:]

PREPARED STATEMENT OF GERALD L. EPSTEIN

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to appear before you today to discuss the Department of Homeland Security's Science and Technology Budget for Fiscal Year 2008. I am currently serving as Senior Fellow in Science and Security in the Homeland Security Program at the Center for Strategic and International Studies (CSIS), here in Washington. I am also an Adjunct Professor at Georgetown University's Edmund A. Walsh School of Foreign Service, where I teach a course on science, technology and homeland security. I have been working in the area of science, technology, and security policy for more than twenty years and have been studying nuclear, chemical, biological, and radiological weapons issues and responses for over 15 years.[1]

At CSIS, my colleagues and I are involved in a major international effort, supported by the Carnegie Corporation of New York and the John D. and Catherine T. MacArthur Foundation, to take a comprehensive, international, and interdisciplinary approach to dissuading, interdicting, mitigating, and responding to biological weapons threats. This project aims to improve the ability to counter these weapons at all stages, from influencing the intent to produce weapons, to denying access to materials and expertise, to detecting illicit programs, to managing the consequences of an attack. The Department of Homeland Security's Science and Technology program, and particularly its biological defense programs, are an important part of the United States'—and the world's—response to these threats.[2]

Other Sources of Advice to Congress

Before I start, however, I cannot help pointing out to this committee that I first started working on the issues I will be discussing today at an agency that no longer exists—the Congressional Office of Technology Assessment. At OTA I was the Project Director for a major series of reports produced for the Congress on the proliferation of weapons of mass destruction, including biological weapons. As much as I welcome the opportunity to discuss these issues with Members of this committee this morning, frankly you and your colleagues deserve more attention than I or any other outside witnesses can devote to you in one hearing. You need a dedicated, credible, and authoritative body of substantive experts, working for you within a carefully structured and fully bipartisan process, that can relate the best available technical understanding directly to the policy choices you face. I have long believed that you and your colleagues—who must act on policy issues that are inextricably dependent on science and technology in practically every Committee of Congress—would find such a capability to be very helpful.

[1] None of the institutions I am affiliated with take policy positions on the topics I will discuss, and the views expressed are strictly my own.

[2] See the CSIS Biological Threat Reduction Program website at *www.csis.org/hs/btr*

Homeland Security Science and Technology Challenges

What we now call "homeland security" has only been recognized as a mission of the Federal Government since the late 1990s, and only since 9/11 has it acquired the resources and organization it has today. Previously, national security policy dealt primarily with overseas threats, and domestic policy did not have a major security component. The U.S. National Academy of Sciences' landmark 2002 study *Making the Nation Safer*[3] recognized the vital role that science and technology could play in bolstering our homeland security, and this report played a significant role in the establishment of a Directorate of Science and Technology within the new Department of Homeland Security (DHS) in 2003. Given both the importance of applying science and technology to this new mission and the paucity of previous government efforts to do so, the DHS S&T Directorate was one of the few parts of the new Department to receive a substantial infusion of new funding; most of the rest of the Department consisted of agencies whose staffs, budgets, and missions were transferred (either whole or in part) from elsewhere in government.

The Department of Homeland Security's Fiscal Year 2008 budget request marks only the fourth one that has been prepared by the Department itself, as opposed to its various predecessor agencies, and applying science and technology to the homeland security mission continues to pose challenges:

1. *Military technology is not directly applicable to homeland security.* Although the military has considerable experience in developing and fielding technologies that are relevant to homeland security needs (such as detecting chemical and biological agents), few military systems can be directly adopted in a homeland security context. Military and civil users differ in their threat scenarios; levels of user skill, experience, and training; systems for maintenance, logistics, and self-protection; sources of funding; willingness to tolerate disruption; ability to issue orders; and respective legal and policy contexts in ways that make it very difficult to use military systems for homeland security purposes. The independent existence of a DHS Science and Technology program is an acknowledgment of this fact.
2. *Users of homeland security technologies may not be federal employees.* Many individuals responsible for mitigating, defending against, or dealing with terrorist attacks in the United States—e.g., police officers, emergency medical technicians, subway train operators, operators of critical infrastructures—are not federal employees at all. They work for State, local, and tribal governments or for the private sector, often in organizations that buy equipment "off the shelf" and that have little experience in developing their own systems. They may even be members of the public attempting to protect themselves. These users tend to be highly disaggregated, and they may not have their own funding to purchase and field new technologies.
3. *Users may not even exist yet.* Some key missions of interest to the DHS S&T directorate—including detection of pathogenic biological organisms in the atmosphere, decontamination of wide areas after a major biological attack, or detection of smuggled nuclear weapons in commercial shipping—were nobody's responsibility prior to the creation of DHS. Moreover, technological breakthroughs can provide capabilities that had never been anticipated, and that no institution or entity may currently be in a position to utilize. Although developing technology without a clear sense of what is needed risks wasting time and money, tying R&D programs exclusively to the identified needs of established users can impede our ability to utilize "game-changing" breakthroughs. Sufficiently powerful tools should motivate us to figure out how to use them.
4. *Technologies don't protect us—systems do.* Throwing technology at a problem does not necessarily make us safer. Careful studies are needed to identify systems and concepts of operations that will mitigate, dissuade, expose, or respond to threats; model how effectively these systems will work in different situations; ask how the deployment of such systems might change the nature of the threat; and evaluate how much better off such a system, on balance, will make us. Moreover, the political leaders who will oversee the use of these systems need to become familiar with their capabilities and their limitations.

---

[3] Committee on Science and Technology for Countering Terrorism, National Research Council; *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* (Washington, DC: National Academy Press, 2002). Available online at *http://www.nap.edu/html/stct/index.html*

5. *Prioritization is, and will remain, difficult.* Perhaps the hardest job in developing homeland security technologies is determining which threats to address, deciding how much to spend on countering each, and measuring our progress. Major terrorist attacks are fortunately rare, and we do not have an exhaustive database of prior attacks that will let us predict what the next attacks will look like. Moreover, tracking terrorist plans and capabilities is much more difficult, say, than counting Soviet armored divisions or intercontinental ballistic missiles was. Modeling and systems studies can provide some guidance in allocating our defensive dollars, but they can be very sensitive to assumptions that will be impossible to justify empirically. Improving our methodologies for such decision-making should itself be a high priority, even if in the end, decision-makers will have to rely on subjective judgment.
6. *No magic organizational solution can eliminate inherent overlap among agency missions,* such as those of the Department of Homeland Security and the Department of Health and Human Services (HHS). DHS deals with deliberate attacks, including those involving biological agents and disease. HHS deals with health and disease threats, including those involving deliberate attack. Biological attacks are both health incidents and security incidents, and both DHS and HHS must be involved in countering them. The potential for conflict can never be eliminated, but it can be managed—particularly through open lines of communication, clear delineation of roles and missions, and an awareness of the different contexts in which each agency views this issue.

Biodefense in the FY 2008 DHS Science and Technology Budget

The largest component of the DHS S&T Directorate's budget is the Chemical and Biological Division, which I was asked to address in my testimony. Overall federal responsibilities for biodefense and biosecurity have been specified in policy documents such as Homeland Security Presidential Directives HSPD–9 ("Defense of United States Agriculture and Food,"), HSPD–10 ("Biodefense for the Twenty-First Century"), and HSPD–18 ("Medical Countermeasures against Weapons of Mass Destruction"), which in turn have generated taskings for the Department of Homeland Security. A few aspects of the Department's biological research and technology development program merit particular attention.

Prioritization. As indicated above, one of the key management challenges facing those responsible for developing and deploying homeland security technologies is establishing priorities. At the operational level, this process would consist of identifying performance or readiness goals that characterize the capabilities we need to achieve; measuring how far we are from those goals; and deriving a set of programs (including acquisition, technology development, training and doctrine, etc.) that will close those gaps. This process would also require some way of evaluating which gaps were most important to close, and which programs would be most effective in closing them. Such a process would involve all agencies that had homeland security responsibilities, and it would be updated regularly.

The National Academies' study *Making the Nation Safer* stated that the government did not have the analytic capabilities it needed to inform decision-making,[4] and it called for such capabilities to be created. That work is incomplete. Even with better tools, however, I believe that assessing risk, setting priorities, and measuring progress will be a very difficult job—one that is harder than the equivalent planning process in the Department of Defense, since homeland security vulnerabilities are more diverse and the threats against them harder to evaluate. In the end, however, dollars have to be spent on some things and not on others, and those choices should be informed by analysis to the greatest extent possible.

Biowatch and the Office of Health Affairs. The transfer of operational responsibility for the Biowatch system into the new Office of Health Affairs for FY 2008 budget is a promising development.

The Biowatch system, which samples air in a number of metropolitan areas for the presence of specific biological threat agents, is an example of a system that was deployed before it had true users. We had never had the ability to respond to a bioterrorist attack on a U.S. city in "near real time"—as or shortly after the agents were released—and it was therefore nobody's job to look for attacks on that timescale. Nevertheless, the motivation for the Biowatch system is compelling—to provide sufficient warning to initiate the distribution of medical countermeasures

[4] *Ibid,* p. 21.

before illnesses start to manifest, when those countermeasures can be far more effective.

The combination of a compelling technical rationale with the lack of an obvious user meant that the early deployment of this system outpaced the development of response protocols that involved all the local, State, federal, and non-governmental entities that would have some role in responding to a true attack. In subsequent years, as we have gained experience operating this system, additional work has been done to incorporate Biowatch information more effectively into response planning and decision-making. Even so, it remains an open question whether or not Biowatch will be able to provide early confirmation of a biological attack with a level of confidence that is high enough for public officials to take highly consequential actions such as community-wide distribution of medication.

Exploration of these essential systems issues will be advanced by the transfer of operational responsibility for running the Biowatch system from the DHS Science and Technology Directorate to the new DHS Office of Health Affairs. The S&T Directorate would retain responsibility for technical improvement and next-generation systems. This transfer for the first time identifies a principal federal "user" for the Biowatch system, albeit a surrogate one. The Office of Health Affairs does not itself mount the full response to a biological attack, but it does have the responsibility to work with actual responding agencies at many different levels of government to ensure that the Biowatch capability is effectively utilized. Clarifying operational and research responsibilities for the Biowatch system is a positive step that will improve both the technical prospects and the operational confidence of the system.

Technically, Biowatch has been highly successful. I would never have predicted that over two million Biowatch assays would have been processed by now without any false alarms. This is a very impressive record that helps to build confidence in the system. At the same time, we have seen a number of "true positives"—the detection of actual threat agents in city air samples. In each case, these detections have been attributed to organisms that occurred naturally in the environment, and none of these detections resulted in mobilizing a full response to a fictitious attack. These detections therefore served to validate the system hardware and analysis protocols, and they also proved that our response protocols did not incorrectly assume a detection always meant an attack.

On the other hand, the fact that Biowatch alarms had to be confirmed by actual cases of disease before a full response would have been mounted does raise the question of what the added value of the Biowatch system is. (Note that the response to an alarm might have been different for an agent such as smallpox, which is not found in nature, for which confirmed laboratory detection would be impossible to attribute to natural causes.) As we continue to gain operational experience with Biowatch, it will be essential for the Office of Health Affairs to evaluate the ways in which Biowatch warning information can prove useful, even if it is not sufficient to trigger a full response. Possible uses of such information include heightening our sensitivity to look for individual cases of disease, triggering some initial stages of pharmaceutical distribution, or informing subsequent determination of the scale and scope of a biological attack.

Relationships Between DHS and Other Governmental Agencies. As described above, there is no organizational solution that will eliminate the potential for interagency conflict or confusion over biodefense. As we are exploring at CSIS in our Biological Threat Reduction project, interactions between different professional communities—embodied in the U.S. Government by different government agencies—are an essential aspect of any response to biological threats. Although these interactions will always present challenges, I believe that the Departments of Homeland Security and Health and Human Services are developing appropriate mechanisms for working together.

In the current fiscal year—pending appropriations—and certainly in the coming year, a new agency in the Department of Health and Human Services will appear on the scene with a vitally important role in biodefense: the Biomedical Advanced Research and Development Authority, or BARDA. With the mission of bridging the gap between basic biomedical research and countermeasure procurement, BARDA will play an essential role in building the Nation's capacity to respond to biological attack. But in addition to facilitating the development of specific countermeasures, BARDA will have an additional mission that may prove even more important in the long run—that of promoting innovative technologies that can reduce the time and cost of countermeasure development in general. With biotechnology becoming ever more powerful and more widely available, we will be less and less able to restrict our attention in the future to a short list of threat agents, each with its own lengthy and expensive countermeasure program.

Instead, we have to move towards a flexible, adaptive, and responsive biodefense system capable of dealing with threats in near-real-time. Creating such a system will blur the distinctions between environmental detection, medical diagnosis, prophylaxis, and treatment, making it even more important for the Departments of Homeland Security and Health and Human Services—whose mission delineations currently depend on some of these functional boundaries—to work together effectively. These departments will also need to work with the Department of Defense, whose Transformational Medical Technologies Initiative, funded by the Defense Threat Reduction Agency, also works to shorten and simplify medical countermeasure development.

Time and Risk Horizon of DHS Research. When the Department of Homeland Security's Science and Technology Directorate was first formed, there were so many immediate demands for science and technology that longer-term research was considered an unaffordable luxury. This may have been a necessary decision at the time, but it was not a sustainable one. Failure to invest in longer-term research limits the prospects for future breakthroughs that could dramatically improve DHS's ability to fulfill its mission.

As the S&T Directorate matures, so must its S&T portfolio—which means investing in a portfolio of both near-term and long-term research. I understand that the S&T Directorate's leadership now shares this view. I particularly welcome Admiral Cohen's plans to fund some high-risk but potentially very high payoff projects. A serious pathology that can overtake a technology development program is to become failure intolerant, forcing it to settle on safe bets that are less ambitious than its mission requires. Admiral Cohen will need your support if he hopes to avoid this—you will have to make sure he fails often enough, and to hold him accountable if he doesn't.

Classified Biological Research and Treaty Compliance. Classified research constitutes a much smaller portion of the U.S. biodefense program than many might suspect. The vast majority of U.S. biodefense consists of unclassified research at the National Institutes of Health, which dwarfs *all* Department of Homeland Security biodefense activities, let alone any classified ones. Nevertheless, classified DHS biodefense research will constitute one of the most controversial parts of the U.S. biodefense program. Research that cannot be shared with diverse technical reviewers, independent non-governmental observers, or foreign colleagues will raise questions with respect to technical merit, policy appropriateness, and treaty compliance.

Even more so than in other areas of science, the biological sciences have enjoyed a tradition of openness and international collaboration—and this heavy presumption of openness should continue. Since disease continues to kill millions of people around the world each year, any restrictions on relevant scientific knowledge could have serious consequences. Yet the existence of hostile, witting adversaries that are determined to wreak devastation and that are known to be interested in biological weapons mandates that this openness not be absolute. The U.S. biodefense program would like to avoid serving as the R&D program or the targeting staff for Al Qaeda or any other terrorist group, even while it works to advance science, cure disease, and assure the world that it is abiding by treaty commitments.[5]

Without attempting to do justice to the complexity of this issue, let me make a few observations about both classification and treaty compliance:

- Actions that violate the 1975 Biological Weapons Convention (BWC) also violate similarly worded provisions of U.S. law.[6] Any government employees or contractors who violated the BWC in the course of their job would be subject to criminal prosecution.
- DHS should engage in public outreach to instill confidence that it is appropriately reviewing its biological research activities, including classified activities, for treaty compliance, legal compliance, and consistency with policy.
- No matter how rigorous its internal review policies are, and notwithstanding the involvement of officials who have no connection to the projects being reviewed, an internal DHS compliance process will not be viewed by outside observers as being truly independent. The more widely that DHS activities, including classified ones, can be reviewed by appropriately cleared individuals

[5] See Center for Strategic and International Studies, Commission on Scientific Communication and National Security, *Security Controls on Scientific Information and the Conduct of Scientific Research* (June 2005) for discussion of some of the tensions between security and openness. This paper is available at *http://www.csis.org/media/csis/pubs/0506_cscans.pdf*

[6] *Biological Weapons Anti-Terrorism Act of 1989,* now at Title 18, Section 175 of the United States Code.

outside of DHS and even outside the U.S. Government, the greater the confidence will be that the Department's activities are technically sound and treaty compliant.

- Even if it cannot all be shared with the public, the United States has an interest in sharing information on its biodefense activities with other countries to assure them that it is complying with the Biological Weapons Convention. The fact that the United States has no offensive biological weapons program should allow it to share this information more widely than if it were seeking to protect a military advantage.
- Classified biodefense activities have been accused of triggering a "security dilemma"—of appearing to others as offensive, and therefore stimulating other countries to respond with offensive programs of their own.[7] Independent of the level of empirical support for this proposition—there are certainly examples of state biological weapons programs that proceeded in, or were even prompted by, the *absence* of any perceived bioweapons activities by their adversaries[8]—this argument retains at least theoretical salience as an incentive for openness. However, it is incomplete at best. It is not clear that a country suspecting others of having offensive biological weapons programs would choose to respond with an offensive program of its own; a much more rational response would be for it to improve its defenses. Even more significantly, the argument fails utterly with respect to non-state programs. Al Qaeda's motivation for pursuing biological weapons, for example, has absolutely nothing to do with any suspicion that the United States may have an offensive program.
- The Biological Weapons Convention bans the development of biological agents "of types and in quantities that have no justification for prophylactic, protective or other peaceful purposes."[9] The treaty has no meaning if any conceivable offensive activity is justified as "protective" on the grounds that it is important for defensive purposes to "see what is possible." Although some may worry that classified U.S. biodefense efforts may be doing just that, I believe that the U.S. biodefense program has too much to do to waste resources on such unconstrained speculation, even without treaty restrictions. However, I also believe that a requirement to be protective can be made operational in a treaty compliance review. To justify an activity as "protective," I would argue that it should be shown to specifically increase our ability to protect ourselves—e.g., that its results should directly and materially inform particular decisions, or contribute to particular capabilities, that improve our ability to protect against biological weapons.

Human Resources for Homeland Security Related Science and Technology. One farsighted program run by the DHS Science and Technology Directorate is its Graduate Fellowship program. This program is intended to support outstanding graduate students in technical disciplines that are important to the DHS mission, with the ultimate objective of strengthening the Nation's science and technology community. However, more can be done to attract these Fellows into careers in the homeland security sector.

Fellows are required to attend an orientation program, to participate in a 10-week internship, and to express willingness to accept homeland security-related employment after graduation (although this is not a binding obligation). U.S. citizenship is required, and security clearances are required for many of the internships.

A strengthened S&T community constitutes "a critical advantage in the development and implementation of counter-terrorist measures and other DHS objectives," as the Fellowship's promotional materials explain,[10] but having these Fellows enter the technical community at large upon graduation does not serve the homeland security mission as effectively as if they were to work directly in the homeland security sector. The United States scientific and technical workforce is strongly dependent on foreign nationals, who constitute a significant fraction of each year's graduates in technical disciplines. Many of these highly skilled foreign nationals remain

---

[7] Jonathan Tucker, "Avoiding the Biological Security Dilemma: A Response to Petro and Carus," *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science,* Vol. 4, No. 2 (2006), pp. 196–197

[8] W. Seth Carus and James B. Petro, "Avoiding the Biological Security Dilemma at Our Own Peril: A Response to Tucker," *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science,* Vol. 4, No. 2 (2006), p. 202.

[9] Biological and Toxin Weapons Convention, Article I(1).

[10] "DHS Scholarship and Fellowship Program 2007 Competition Guidelines," *http://www.orau.gov/dhsed/*

in the United States after graduation, to this country's great benefit.[11] However, foreign nationals are not eligible to work in many homeland security-related institutions. DHS Graduate Fellows can, and policies that maximize the fraction of these technically trained U.S. citizens who enter the homeland security sector would be very valuable.

The current program exposes Fellows to DHS problems and processes to some degree, but I think that a deeper level of engagement with these Fellows, with a more thorough exposure to the U.S. Government's homeland security operations, will stimulate greater interest in pursuing homeland security careers after graduation. More should be done to secure security clearances for the Fellows and brief them on homeland security threats at a classified level; to have senior representatives from homeland security and related agencies (i.e., homeland security, intelligence, defense, public health, critical infrastructure) meet with them to describe their jobs, their agencies' responsibilities, and different ways in which science and technology build homeland security capabilities; and to establish mentorships between Fellows and senior employees in the homeland security sector. The Fellows should be convened periodically, perhaps by holding regional meetings or seminars that would be convenient for them to attend. Ongoing engagement with the Fellows is much more likely to elicit an interest in a career in homeland security than a single orientation.

A model for such a program of continuous engagement and involvement of technical professionals in security problems, albeit one pitched at a smaller number of individuals at a more senior level in their career, would be the Defense Science Study Group that is organized by the Institute for Defense Analyses for DARPA. I would recommend that DHS officials involved in the Graduate Fellowship Program familiarize themselves with that activity.

Mr. Chairman and Members of the Subcommittee, I thank you for your interest, and I would be pleased to answer any questions you may have at this time.

BIOGRAPHY FOR GERALD L. EPSTEIN

Gerald Epstein is Senior Fellow for Science and Security in the CSIS Homeland Security Program, where he works on issues including reducing biological weapons threats, improving national preparedness to respond to biological attack, and ameliorating tensions between the scientific research and national security communities. He is also an Adjunct Professor with the Security Studies Program at Georgetown University's Edmund A. Walsh School of Foreign Service, where he teaches a course on "Science, Technology, and Homeland Security." Epstein came to CSIS in 2003 from the Institute for Defense Analyses, where he had been assigned to the Defense Threat Reduction Agency. From 1996 to 2001, he worked at the White House Office of Science and Technology Policy (OSTP), serving for the last year in a joint appointment as Assistant Director for National Security at OSTP and Senior Director for Science and Technology on the National Security Council staff. His responsibilities at OSTP included technologies to counter terrorism and to protect the Nation's critical infrastructures; chemical and biological weapons nonproliferation and arms control; missile defense; strategic arms control; the nuclear weapon stockpile stewardship program; export controls; and national security/emergency preparedness telecommunications.

From 1983 to 1989 and again from 1991 until its demise in 1995, Dr. Epstein worked at the Congressional Office of Technology Assessment, where he directed a study on the proliferation of weapons of mass destruction and worked on other international security topics. From 1989 to 1991, he directed a project at Harvard University's Kennedy School of Government on the relationship between civil and military technologies, and he is a co-author of *Beyond Spinoff Military and Commercial Technologies in a Changing World* (Boston, MA: Harvard Business School Press, 1992). He has also served as visiting lecturer in public and international affairs at Princeton University's Woodrow Wilson School.

Dr. Epstein is a Fellow of the American Physical Society and in 2007 chairs that society's Committee on International Scientific Affairs. He is also a member of the editorial board for the journal *Biosecurity and Bioterrorism* and of the Biological Threats Panel of the National Academy of Sciences' Committee on International Security and Arms Control. He received S.B. degrees in physics and electrical engi-

---

[11] See Center for Strategic and International Studies, Commission on Scientific Communication and National Security, *Security Controls on the Access of Foreign Scientists and Engineers to the United States* (October 2005) for discussion of the importance of foreign interchange to the U.S. science and technology base. This paper is available at *http://www.csis.org/media/csis/pubs/051005_whitepaper.pdf*

neering from MIT and a Ph.D. in physics from the University of California at Berkeley.

Center for Strategic & International Studies
Washington, DC

March 5, 2007

The Honorable David Wu
Chairman, Subcommittee on Technology and Innovation
Committee on Science and Technology
Suite 2230 Rayburn House Office Building
Washington, DC 20515-6301

Dear Chairman Wu:

I am pleased to accept your invitation to testify before the Subcommittee on Technology and Innovation on Thursday, March 8, 2007.

This letter constitutes my Conflict of Interest statement, which I interpret to address funding I receive or have received, through CSIS or in my individual capacity, from the Department of Homeland Security (DHS) Science and Technology Directorate. I do not know whether there are other people at CSIS who are in part supported by DHS, although it would not surprise me.

1. At CSIS, I am currently working on a subcontract to the Department of Homeland Security, through the Homeland Security Institute, which addresses the topic of decontamination after a biological attack. I believe that the funding for this subcontract originates in the Chemical and Biological Division of the DHS Directorate of Science and Technology.
2. In past work at CSIS, I had worked on a different subcontract to the Department of Homeland Security (also through the Homeland Security Institute) on the topic of international cooperation in homeland security science and technology. This subcontract, which was funded by the DHS Directorate of Science and Technology, has been completed.
3. In past work as my individual capacity, I have worked on projects for contractors that I believe were funded by the Department of Homeland Security, although I do not believe they were funded by S&T Directorate.
4. I am not aware of additional projects that others within my institution are performing for the Department of Homeland Security. However, I do expect that I may find myself working on tasks funded by the DHS Directorate of Science and Technology in the Future.

Please contact me at 202-775-3125 or by email at gepstein@csis.org if you have any questions.

Sincerely,

Gerald L. Epstein
Senior Fellow for Science and Security

1800 K Street Northwest • Washington, DC 20006 • Telephone 202/887-0200 • FAX 202/775-3199 • WEB: http://www.csis.org/

Chairman WU. Thank you, Dr. Epstein. Mr. Czerwinski.

STATEMENT OF MR. JONAH J. CZERWINSKI, MANAGING CONSULTANT, IBM GLOBAL BUSINESS SERVICES; SENIOR FELLOW, HOMELAND SECURITY, IBM GLOBAL LEADERSHIP INITIATIVE

Mr. CZERWINSKI. Chairman Wu, Ranking Member Gingrey, Congressman Mitchell, my name is Jonah Czerwinski. I am a senior fellow with IBM's Global Leadership Initiative and a managing consultant at IBM's Global Business Services. I thank you for the opportunity this morning to appear before you to highlight three things.

First, IBM's dedication to supporting basic research and services science. Second, the investment priorities of the DHS Domestic Nuclear Detection Office, and the importance of placing these efforts in a broader framework that protects the golden flow of trade and travel. And third, matching R&D investments of the DNDO to the risks posed by covert nuclear weapons and materials.

IBM spends approximately $6 billion per year on research and development. Much of it on basic research. However, increasingly IBM and others are also investing in research in emerging areas such as services, which comprise approximately 80 percent of the U.S. economy and account for more than 75 percent of IBM's corporate revenues. We believe that the national investment in basic research remains critical to foster innovation and to support our country's economic competitiveness. And we advocate that the Federal Government also should support research and curriculum development in the area of services science.

By way of background from 2004, through the early part of this year I was director of Homeland Security projects at the Center for the Study of the Presidency and worked with Center President David Abshire and Norm Augustine to organize the Nuclear Defense Working Group. That group provided the groundwork and rationale for the Government reorganization that led to the Domestic Nuclear Detection Office.

The challenge of nuclear material is its subtle radiological signature, which usually requires a detector to be both close to the suspected source and within its vicinity for enough time to gather telltale radiation. For this reason most of the investments made in detecting smuggled nuclear weapons should support two key success factors; increasing distance between the detector and the radioactive material and decreasing dwell time near the material itself.

The DNDO budget includes funding for certain longer-term R&D commitments that show progress in these areas. For example, the development of the Advanced Standoff Detection Program that Mr. Oxford described could become a game-changing capability. This research may deliver faster detection at a greater distance.

In the end, investments like these must not only protect the public and the Nation's critical assets but do so without harming the flow of trade and travel. Congress must view the effort to combat the smuggled nuclear weapons threat as one of several interlocking objectives, many of which should benefit from our R&D investments. Doing so requires a framework that connects the search for global, excuse me, the search for nuclear materials to the broader

goal of protecting the flows of cargo, people, and conveyances in the global trade and travel system. The DNDO should figure prominently in this mission.

Ultimately, homeland security R&D investments should support the broader objective of bringing efficiency, security, and resilience to one of the most attractive targets of WMD terrorism; the flow of global trade and travel. IBM has developed a means by which today's homeland security imperatives can reinforce both efficiency and security in the global movement of cargo, people, information, and finance. We call this framework Global Movement Management. It adds resilience to this critical system of movement without imposing inefficiencies that risk outweighing the security benefits to the numerous stakeholders that use these systems of trade and travel. The country needs a strategic framework like you mentioned to overarch our R&D investments for maximum benefit to both our Homeland Security interests and our economic competitiveness.

The strategic framework is lacking today. Nevertheless, DNDO has chosen successfully several important pilots, including those I mentioned in my written statement.

This leads me to my final point. Mr. Chairman, you asked specifically about the role of risk assessments and identifying the best use of our R&D investments in this area. When the DNDO first was created, it was understood by its authors that as the threat of nuclear terrorism and proliferation would evolve, America's relevant technological base would evolve and would other significant international factors such as the war in Iraq and Afghanistan. It was, therefore, critical that as a help for national efforts to combat the smuggling of nuclear material, the DNDO began with a net assessment of the Nation's capabilities, matched against a current snapshot of the threat. The DNDO's Global Nuclear Detection architecture is based on that assessment. It includes guidance on how best to operate the nuclear detection assets and authorities, as well as a clear list of gaps in America's nuclear detection efforts. Those gaps lead to DNDO's list of investment priorities.

I would recommend giving special attention to the methodology and makeup of the Global Nuclear Detection architecture to better illustrate the connection between risk and the DNDO's budget. Ultimately, these individual investments can serve a greater goal of resilience, security, and efficiency. The DNDO and the Executive Branch as a whole should be measured by the ability of their R&D investments to do just that.

Thank you very much. I look forward to your questions.

[The prepared statement of Mr. Czerwinski follows:]

PREPARED STATEMENT OF JONAH J. CZERWINSKI

Chairman Wu, Ranking Member Gingrey, Members of the Subcommittee, I am pleased to appear before you today to comment on the role of the Department of Homeland Security's (DHS) Domestic Nuclear Detection Office (DNDO) in securing the homeland against the smuggled nuclear threat, the DNDO's budget priorities, and the extent to which this relatively new office works across the interagency and with relevant partners and stakeholders outside of the federal government.

I am a Senior Fellow with IBM's Global Leadership Initiative[1] and a Managing Consultant for IBM's Global Business Services. I am here to address three items. First, I will discuss select high-leverage and innovative components of the DNDO's budget that I believe strike the right balance between immediate deployment and the vital long-term commitment to basic research. Second, I will address the need for investing in a reorganization that is currently underway at DNDO that reflects its crosscutting mission. And third, I will place this mission in the broader context of a framework that connects the defense against smuggled nuclear materials to the imperative of protecting the stream of cargo, people, conveyances, information, and money flows in the global trade system.

IBM has invested in the development of new thought leadership in this field because we, like the Members of this committee, value innovation. Innovation is the key to our competitiveness—both IBM's and the Nation's. IBM spends approximately $6 billion per year on research and development (R&D)—much of it on basic research. However, increasingly, IBM and others also are investing in research in emerging areas such as services, which, as you may be aware, make up approximately 80 percent of U.S. economy, while employing approximately the same percentage of the U.S. labor force. As a country, we need to invest in the skills needed for 21st century jobs that will almost certainly be dominated by the services market. This means funding investment in the emerging academic discipline of services science, including R&D and curriculum development.

My own work at IBM focuses on developing a comprehensive framework for security, resilience, and efficiency in the global movement of goods, people, and information. From 2004 through the early part of this year, I was Director of Homeland Security Projects at the Center for the Study of the Presidency.[2] Beginning in April 2004, I worked with Center President David Abshire to organize the Nuclear Defense Working Group. That group provided the groundwork and rationale for a government reorganization that led to the creation of the Domestic Nuclear Detection Office.

Origins and Initiatives of the DNDO

The single most devastating threat to America remains a nuclear weapon covertly detonated in a major city. Presidents have considered this risk ever since Einstein wrote Franklin Roosevelt in 1939 to warn him that a "bomb of this type, carried by a boat and exploded in a port, might very well destroy the whole port together with some of the surrounding territory."[3] While that risk is much greater today than it was then, some progress in the field of detection has been made.

In April 2004, a talented group of experts gathered at the Center for the Study of the Presidency to consider an intimidating question: Is the Nation doing all that it can to reduce the risk of covert nuclear attack at an acceptable cost? Norman Augustine co-chaired the session with then-Deputy Secretary of Homeland Security, Admiral James Loy. Representatives from the Departments of Defense, Energy, and Homeland Security, along with participants from the White House, national laboratories, and think tanks attended.

Two perspectives emerged during that meeting. One held that highly enriched uranium (HEU) or plutonium used in a nuclear weapon is simply too difficult to detect because of the low radiation levels they emit prior to detonation. The other argued that today's technology simply lacks the strength to detect an element as subtle as HEU, but improvements are not impossible. Both groups agreed that, among other things, a better organization within government was necessary to improve detection because existing national efforts simply were too disunified.[4] Solving the political science problem would help solve the physical science problem.

The result was the creation of the DNDO in April 2005 through Homeland Security Presidential Directive 14.[5] The DNDO was born out of the acknowledgement that no single agency had the assets, authorities, or responsibilities needed to address the risk of covert nuclear attack. Since then, this office, under the leadership of Vayl Oxford, and the reorganization of DHS's Science and Technology Directorate,

---

[1] The Global Leadership Initiative is a strategy team designed to cut across all IBM business lines to identify new ideas that place IBM at the forefront of companies with the ability to anticipate and serve customer needs in the public sector on a global basis.

[2] The Center for the Study of the Presidency is a non-partisan, non-profit organization founded in 1965 to examine past successes and failures of the Presidency as they apply to present challenges and opportunities.

[3] Albert Einstein, Leo Szilard correspondence to President Franklin D. Roosevelt. August 2, 1939.

[4] See "Report of the Defense Science Board Task Force on Preventing and Defending Against Clandestine Nuclear Attack." *http://www.fas.org/irp/agency/dod/dsb/attack.pdf.*

[5] The text of HSPD 14 can be viewed at *http://www.fas.org/irp/offdocs/nspd/nspd-43.html.*

led by Under Secretary Cohen, have led to significant progress in combating the threat of terrorism.

Over the past two years, the DNDO has stood apart as a work in progress and as a place for addressing one of the Nation's most urgent security concerns. While the DNDO is still nascent, it is no longer "too early to tell" if it is achieving its goal of integrating and accelerating national efforts to combat the smuggled nuclear weapons threat.

Mr. Chairman, your invitation to testify before this committee included the important indicators to gauge the success of this experiment: Does the new budget request—the third for this office—advance the highest priorities for combating smuggled nuclear weapons? Do those priorities reflect an adequate read of the risk? Are current research efforts producing results that support the DHS mandate? Is DNDO collaborating effectively with other federal agencies?

When the DNDO first was created, it was understood by its authors that as the threat of nuclear terrorism and proliferation would evolve, America's relevant technological base would evolve, as would other significant international factors—such as the wars in Iraq and Afghanistan and Nunn-Lugar programs. It was therefore critical that, as a hub for national efforts to combat the smuggling of nuclear material, the DNDO begin with a net assessment of the Nation's capabilities matched against a current snapshot of the threat.

The DNDO's "Global Nuclear Detection Architecture" is based on that assessment. It includes guidance on how best to operate the nuclear detection assets, authorities, and responsibilities. What emerges is a clear list of gaps in America's covert nuclear detection capabilities. Those gaps lead to the DNDO's list of priorities.

The Global Nuclear Detection Architecture is an interagency product designed to provide a plan for improving the status quo through a deliberate systems engineering approach to a gradual—and perhaps someday rapid—reduction of the risk of covert nuclear attack. Its success depends upon a multilayered system of systems that must knit together initiatives contributing to a reduction of the risk in the U.S., across the maritime and air domain, and in foreign territories.

DNDO priorities reflect a shared perception of the threat as it evolves over time. The real challenge is setting a budget that balances the imperative of deploying available detection capabilities now with conducting basic and applied research that push the limits of today's technology and help create new capabilities for tomorrow. Interwoven with that strategy is a more strategic asset: an integrated forensics mission that reaches across the U.S. Government.

To adequately combat the risk of smuggled nuclear material, the DNDO invests in exploratory research that challenges assumptions about the limits of technology. It takes the gaps in the Global Nuclear Detection Architecture and makes longer-term R&D commitments to promising solutions. These efforts can lead to major game-changing improvements in our ability to combat nuclear terrorism. Some promising examples include the following:

1) First, the FY08 budget request includes about $12 million for a technology demonstration called the Verification of Shielded Special Nuclear Material (SNM). This initiative addresses the risk caused by a proliferator or perpetrator who seeks to foil many currently deployed detectors by moving critical bomb-making material while hiding it behind lead or other shielding.
2) Second, the budget includes about $11 million for the Intelligent Personal Radiation Locator, or IPRL. The technology represents a move from search to surveillance, and it amounts to a transformation of the current version of the "pager" devices now used, which are little more than personal Geiger counters. The IPRL investment addresses, albeit in a limited way, the gap that was identified in the Global Nuclear Detection Architecture showing the need for increased numbers of smaller, more mobile detectors to help locate stolen nuclear material or weapons at a late stage of deployment. The new locators—presently at a very early demonstration stage—are worn on a belt and can provide the wearer with indications of where the source is located and the type of isotope within range. They also have the ability to communicate wirelessly with other locaters so as to rapidly close in on a suspicious source. All of this is done with increasing range and with greater reliability.
3) Third, the DNDO is developing the advanced Stand-off Detection capability, which focuses on increasing the distance from dangerous nuclear material while decreasing dwell time near that material. Both are critical. However, the challenge of nuclear material is its subtle radiological signature, which usually requires a detector to be both close to the suspected source and in its vicinity for enough time to gather telltale radiation. By soliciting competing teams of partners among private industry, national laboratories, and

academia, this research may deliver more detailed imaging capabilities at a range that is increased by a factor of 10 or more. This same effort could produce detectors capable of working effectively, while moving at a rate of 20 miles per hour. The result of faster detection at a greater distance from the source material—combined with intelligence tools for better targeting—will not only protect the public and the Nation's critical assets, but it also will facilitate the movement of cargo through ports without sacrificing security.

4) Fourth, the FY2008 budget request includes $16.9 million for the National Technical Nuclear Forensics Center (NTNFC), which supports DNDO's technical forensics responsibility. This money would support not only an R&D investment, but also a much-needed reorganization. Nuclear forensics cuts across the entire mission space from deterrence and dissuasion, to detection through consequence management, to attribution and response. It is a core part of the mission of combating smuggled nuclear weapons.

The NTNFC should be considered a priority given the significant return on investment that progress in this area can deliver. While the Department of Homeland Security is not responsible for the entire spectrum of forensics, the NTNFC represents a step forward in two clearly needed capabilities:

1. Across the government, unify various competencies and programs that are focused on aspects of the forensics mission.
2. Develop, enhance, and maintain technical forensics capabilities for pre-event needs.

DNDO Collaboration

This committee asked specifically whether the DNDO is collaborating effectively with other federal agencies. I believe that combating the smuggled nuclear weapons threat is, by nature, a collaborative mission. This mission was at the center of the interagency debates in 2004, and the DNDO of today reflects this imperative. This is an area in which the DNDO has made progress.

Since the National Technical Nuclear Forensics Center is in many ways a microcosm of the DNDO, I would like to highlight a few examples here that represent a broader collaborative effort now underway. At the NTNFC, the FBI provides an expert as Deputy Assistant Director, and it also provides a senior liaison from the FBI lab. The Department of Defense provides a detailee, and the Department of Energy is assigning an expert of its own.

The Forensics Center has a Working Group, made up of members from each relevant federal agency and members of the intelligence community, which meets regularly to address high priority issues. There is an "Interagency NTNF Program & Budget Crosscut" that is under development to help align relevant programs and harmonize budget requests. Lastly, the NTNFC—and the DNDO in general—work with interagency partners in planning and executing exercises that support the research, development, and deployment of technologies, as well as shared concepts of operations, or CONOPS.

DNDO works mostly with the Department of Energy's (DOE's) Office of Nonproliferation Research and Development, known as NA–22, and DOD's Defense Threat Reduction Agency. The interactions include serving as proposal evaluators on each other's programs, deconflicting projects by comparing portfolios, and jointly participating in project reviews and technical reports.

The Advanced Technology Demonstrations (ATDs), such as Standoff Detection and Verification of Shielded Nuclear Material, include teams that have developed technology with funding from DNDO, DOE, DOD, and other sources. The purpose of an ATD is to develop and test a technology that addresses a critical need and which has reached a proof-of-concept stage, usually with payoff for more than one agency. In this way, DNDO takes advantage of work that is funded by others, but it also supports R&D that can be useful to other agencies.

For example, some efforts at DNDO could contribute to Maritime Domain Awareness (MDA)[6], a major program developed by the Coast Guard to identify threats and intercept them before they arrive onshore. In MDA, the Coast Guard and Department of Defense require better intelligence, as well as detection and interdiction

[6] MDA is the principle strategy articulated in "The National Plan to Achieve Maritime Domain Awareness," which was released by the Department of Homeland Security in October 2005. As directed by National Security Presidential Directive-41/Homeland Security Presidential Directive-13, it is one of eight plans developed to support the National Strategy for Maritime Security.

capabilities to accomplish their goals. In the context of nuclear terrorism, a successful mission depends upon the ability to detect threatening material or people at the greatest possible distance. The ability of DNDO to contribute to that mission should be a measure of its return on investment.

Placing Detection R&D Within a Broader Framework

Congress must view the effort to combat the smuggled nuclear weapons threat as one of several interlocking objectives, many of which should benefit from R&D investments. Doing so requires a framework that connects the search for nuclear materials to the broader flows of cargo, people, conveyances, information, and money in the global trade and travel system. And that framework should reach across DHS, DOD, DOE, State, and other departments to improve the resilience and security of the global trade and travel system, while ensuring its security.

The DNDO—and DHS S&T—should figure prominently in this mission. Ultimately, the federal R&D management process must more effectively link the strategic planning process at DHS with the broader mission of bringing transparency, efficiency, security, and resilience to one of the most attractive targets of WMD terrorism: the global flow of trade and travel.

IBM has developed a framework like this that also acknowledges an existing incentive for the private sector, which is to satisfy the economic imperative to improve the efficient and reliable flow of people, cargo, conveyances, money and information.

At IBM, we call this framework "Global Movement Management."[7] It is a means by which the technology requirements of today's homeland security measures can provide for both efficiency and security in the global movement of cargo, people, information, and finance. This new framework adds resilience to this critical system of movement without imposing inefficiencies that risk outweighing the security benefits to the numerous stakeholders that use these systems of trade and travel.

For the DNDO, finding a smuggled nuclear weapon on a ship in the Port of Portland is too late. That threat must be identified, verified, and interdicted before it ever approaches. The DNDO investments that I highlighted go a long way in generating the transparency needed to identify a threat, but the broader strategy should consider, in this example, that the shipping system itself must be able to withstand a disruption, terrorist or otherwise. This is because, as global movement becomes ever more interdependent, a disruption—let alone an actual attack—would be catastrophic.

Conclusion

The country needs a strategic framework to overarch our R&D investments for maximum benefit to both our homeland security interests and our economic competitiveness. DNDO and DHS lack this strategic framework today. Nevertheless, DNDO has chosen successfully several important pilots, including those I mentioned. Indeed, Congress should view DNDO's work as being on track after three years.

But Congress also should consider how the individual investments can serve a greater goal of resilience, security, and efficiency. The DNDO, and the Executive Branch as a whole, should be measured by the ability of their R&D investments to do just that.

Thank you. I would be happy to respond to any questions that you may have.

BIOGRAPHY FOR JONAH J. CZERWINSKI

Jonah Czerwinski is Managing Consultant, Global Business Services at IBM, working on homeland security policy issues, and he is a Senior Fellow in IBM's Global Leadership Initiative. Jonah is also a Senior Advisor for the Center for the Study of the Presidency and a 2007 Senior Fellow at the Homeland Security Policy Institute of George Washington University.

From 2003 to 2006, Jonah was Senior Research Associate and Director of Homeland Security Projects at the Center for the Study of the Presidency (CSP). He led the Center project on combating the smuggled nuclear threat, which worked across the Executive Branch in an effort that led to establishment of the Department of Homeland Security's National Domestic Nuclear Detection Office (DNDO). He also served on the Council on Foreign Relations Study Group on Strategies for Defense Against Nuclear Terrorism. From 2001–2004, he directed the Center's Homeland Se-

[7] Global Movement Management (GMM) is a comprehensive governance structure and system architecture for monitoring and securing the key flows of global commerce—people, goods, conveyances, money, and information. It provides the framework to safeguard the global economy against disruptive threats by fostering new levels of visibility, accountability, and resiliency.

curity Roundtable, which regularly convened senior Homeland Security leadership of the Executive Branch and Congress with leaders of the think tank community, academia, and private sector to discuss critical Homeland Security issues.

Jonah led a Center project on strengthening the transatlantic relationship through NATO, which published *Maximizing NATO in the War on Terror* in May 2005. He also directed the Center's working group on *The U.S.-Canada Strategic Partnership in the War on Terrorism* in 2002. He served as a member of the "Taskforce for Examining the Roles, Mission, and Organization of the U.S. Department of Homeland Security," which published its recommendations as *DHS 2.0* (December 2004). In 2005, he was Senior Fellow at the Homeland Security Policy Institute of George Washington University, and in 2004, he was named a Manfred Wörner Fellow.

Jonah was a contributing writer to and research coordinator of the Center's 2001 report on *Comprehensive Strategic Reform.* He was project coordinator and principal writer of *Forward Strategic Empowerment: Synergies Between CINCs, the State Department, and Other Agencies,* and assistant editor and contributor to *In Harm's Way: Intervention and Prevention.*

Professional media appearances include interviews on CNN and CNN–International, in addition to interviews for *The New York Times, Wall Street Journal, The National Journal, Los Angeles Times, Congressional Quarterly, National Defense,* and other major news outlets. In addition to authoring, editing, or co-authoring a number of publications, Mr. Czerwinski has spoken at the Elliott School of International Affairs at The George Washington University, the Center for International Security Studies at the University of Maryland, and the graduate school at Salve Regina University.

Prior to joining the Center in late 1999, Mr. Czerwinski was an analyst with the program in International Finance and Economic Policy and a research assistant to the CEO at the Center for Strategic and International Studies (CSIS). He has worked with the George Washington University Center for International Health on the intersection of international security and health, as a consultant to CSIS, and as coordinator for the Trinity National Leadership Roundtable. He serves on the Advisory Council of the Salvation Army of Washington, DC, as Chairman of the Nominating Committee. Mr. Czerwinski earned his undergraduate degree (A.B., Philosophy) from Salve Regina University.

Chairman WU. Thank you very much, Mr. Czerwinski. Ms. Ward.

STATEMENT OF MS. MARILYN WARD, EXECUTIVE DIRECTOR, NATIONAL PUBLIC SAFETY TELECOMMUNICATIONS COUNCIL (NPSTC)

Ms. WARD. Chairman Wu, Ranking Member Gingrey, and the Members of the Subcommittee, on behalf of the National Public Safety Telecommunications Council, referred to as NPSTC, it is a privilege to appear before the Subcommittee and its examination of the Department of Homeland Security's research and development activities. We commend the Subcommittee's work in this area.

NPSTC's mission is devoted to improving the communications capabilities of local and State public safety agencies. NPSTC was created in 1997, as a volunteer federation of 13 national public safety associations. Our efforts are focused on the technological capability and the capacity of radio communications and the coordination of these resources throughout all agencies.

The following are just a few examples of what NPSTC does. We provide the DHS SAFECOM Program local and State public safety input to its Science and Technology research and development and standard efforts. NPSTC critically examines technical and regulatory implications regarding radio spectrum utilization and management.

NPSTC provides comments to the FCC on critical public safety issues representing over 250,000 public safety responders. NPSTC

provides an open forum for discussion and dispute resolution on public safety communications issues.

My testimony today focuses on the DHS Science and Technology role in furthering public safety communications. Through its Executive Committee, Emergency Response Committee, and organizations like NPSTC, SAFECOM is developing a national plan to enhance inter-operability.

We believe the focus on new and innovative technology today is found in broadband. The challenge is that public safety spectrum is currently not available for a nationwide broadband network that is controlled by and built to public safety standards and requirements. The recent testimony of Chief Harlan McEwen from IACP, the International Association of Chiefs of Police, and Chief Charles Werner of the International Association of Fire Chiefs, to the Senate Commerce Committee is supported by all of the major public safety associations, including NPSTC, and it is attached to my written testimony.

The public safety community is concerned that there was considerable reduction in the 2007 budget and that the newly created Office of Emergency Communications was left unfunded. Agencies transferring portions of their budgets to fund DHS OEC is time-consuming, it creates tension among agencies, and causes confusion and uncertainty for the State and local community.

DHS SAFECOM has pursued development of regional radio systems by soliciting participation using a bottom-up strategy. Although this takes time, it is a critical element and must be completed. In addition to the tools and critical studies SAFECOM develops, they also test, evaluate technologies, conduct pilot programs, and are funding a compliance lab. None of these have adequate resources.

Although not directly involved with the Department's planning and priority mechanisms, we do not see projects and programs based on long-term solutions to the problems that we face in communications. The budgets at the federal level fluctuate and are not sustained in a manner that is conducive to long-term solutions.

DHS SAFECOM, along with their partners at the National Institute of Standards and Technology, Office of Law Enforcement Standards, and the National Telecommunications and Information Agency Institute for Telecommunication Sciences are currently testing the current public safety standard commonly referred to as P25. This is an especially important requirement because many of the State and local agencies, as well as the Department of Defense and other federal agencies, are using P25 equipment. Through the SAFECOM Program, NPSTC has been involved with the NIST/OLES for many years such as in the development and review of the SAFECOM Statement of Requirement for public safety communications technology.

Another example of our collaboration occurred last month when NPSTC worked with NTIA ITS in Bolder to develop requirements for broadband technologies. Through this collaboration the original input of 57 practitioners was expanded to 627 who provided input to the project.

I would also like to ask that this subcommittee review our comments on the progress made regarding the recommendations of the

September 2004, GAO report on inter-operability, which is provided in my written testimony.

In closing, there are two issues the Subcommittee and Congress should consider. First, fluctuations in funding for communications inter-operability deters progress. Three to five-year funding estimates would provide stability for long-term programs and strategies and would result in considerably more improvements.

The second issue we would like you to consider is the proposal to permit the creation of a Public Safety Broadband Trust in the 700 MHz and reallocating 30 MHz of spectrum to public safety that is scheduled to be auctioned. We urge Members to examine this issue very closely. It would make a positive and important contribution to public safety communications.

Thank you, again, for the invitation to appear before this committee.

[The prepared statement of Ms. Ward follows:]

PREPARED STATEMENT OF MARILYN WARD

Chairman Wu, Ranking Member Gingrey, and Members of the Subcommittee:

On behalf of the National Public Safety Telecommunications Council (NPSTC), it is a privilege to appear before the Subcommittee in its examination of the Department of Homeland Security's Research and Development Activities. NPSTC's mission is devoted to improving the communications capabilities of local and State public safety agencies. With heightened domestic defense and emergency response demands, the work of the Department of Homeland Security in this area is vital.

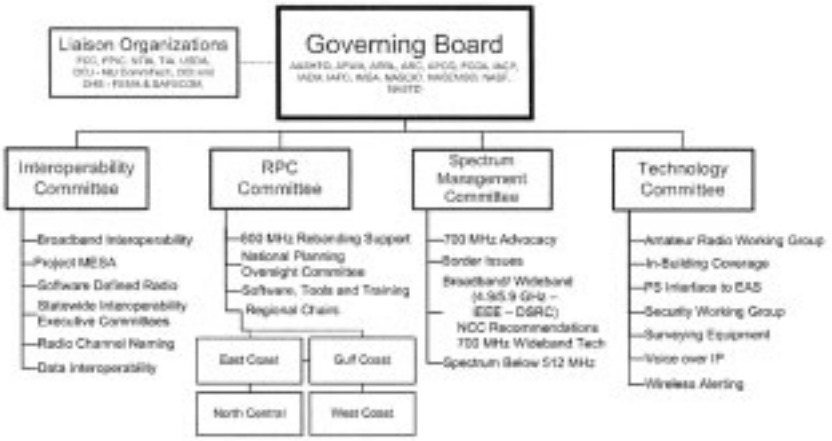
NPSTC was created in 1997 as a volunteer federation of associations representing State and local public safety telecommunications to advance communications capabilities, including inter-operability, of first responders, through one collective voice for public safety communications. NPSTC serves both as a resource and advocate for public safety organizations in the United States on matters relating to public safety telecommunications. The technical capability and capacity of radio communications and the coordination of these resources across all agencies are fundamental to our core mission, that of speeding response to the citizen facing an emergency.

NPSTC is dedicated to encouraging and facilitating, through its collective voice, the implementation of the Public Safety Wireless Advisory Committee (PSWAC), and the 700 MHz Public Safety National Coordination Committee (NCC) recommendations. NPSTC explores technologies and public policy involving public safety agencies, analyzes the ramifications of particular issues, and submits comments to governmental bodies with the objective of furthering public safety communications worldwide. NPSTC serves as a standing forum for the exchange of ideas and information for effective public safety telecommunications. The following 14 organizations participate in NPSTC:

American Association of State Highway and Transportation Officials
American Radio Relay League
American Red Cross
Association of Fish and Wildlife Agencies
Association of Public-Safety Communications Officials-International
Forestry Conservation Communications Association
International Association of Chiefs of Police
International Association of Emergency Managers
International Association of Fire Chiefs
International Municipal Signal Association
National Association of State Chief Information Officers
National Association of State Emergency Medical Services Officials
National Association of State Foresters
National Association of State Telecommunications Directors

Several federal agencies are liaison members to NPSTC. These include the Department of Agriculture, Department of Homeland Security (SAFECOM Program, and the Federal Emergency Management Agency), Department of Commerce (National Telecommunications and Information Administration), Department of the Interior, the Department of Justice (National Institute of Justice, CommTech Program), and the Federal Communications Commission (FCC).

Below is an illustration of the NPSTC organization, its four operational committees and multiple working groups. It is clear that there are many topics to be resolved that impact public safety communications and NPSTC is active in developing positions and advocating for State and local first responders.



NPSTC IS AN ADVOCATE FOR PUBLIC SAFETY COMMUNICATIONS IN THE FOLLOWING WAYS:

NPSTC is the only national consensus forum for major public safety associations that facilitates an open dialog and exchange of information on critical public safety telecommunication issues.

NPSTC provides the SAFECOM Program local and State public safety communications input to science and technology research and development projects and related standards efforts.

NPSTC critically examines technical and regulatory implications regarding radio spectrum utilization and management.

NPSTC provides comments to the FCC on critical public safety issues upon receiving consensus from its 14 member associations, representing over 250,000 public safety responders.

NPSTC's members include the four FCC certified public safety frequency coordinators.

NPSTC includes liaisons from the Federal Government that ensure feedback to and from practitioners and policy-makers.

NPSTC provides an open forum for our members, guests and the community for discussion and dispute resolution, including the ability for people who cannot travel to attend the meetings by calling into a teleconference bridge.

NPSTC actively engages in securing and protecting spectrum for states and localities: 700 MHz for Wide Area Voice and Data, 800 MHz Rebanding, continued VHF & UHF availability and 4.9 GHz for on-site broadband.

NPSTC actively monitors key technology-related issues having long-term implications on public safety inter-operability by actively participating in Software Defined Radio forums (SDR), International Association of Electrical and Electronics Engineers (IEEE) meetings, and international public safety standards efforts, such as Project MESA.

NPSTC addresses public safety spectrum issues along the U.S. border by participating in related State Department efforts.

NPSTC provides the SAFECOM Program a forum to monitor the pulse of the public safety community and determine needs to improve inter-operability.

NPSTC recently developed a common radio channel naming plan to standardize the radio channels to read the same display no matter where the responder is located in the U.S.

NPSTC is currently developing a dispute resolution procedure for 700 MHz Regional Planning Committees when conflicts occur among adjacent regions.

NPSTC monitors 4.9 GHz and 5.9 GHz testbeds and communicates the information to the State and local public safety community.

NPSTC communicates the impact and solutions of nationwide reviews of in-building radio coverage to the public safety community.

NPSTC promotes a national forum where Amateur Radio and public safety work together on nationwide public safety wireless communication issues.

As the founding Chair and current Executive Director of NPSTC, I would like to convey to the Subcommittee how important its work is and relate our appreciation for inviting us to speak on the issues that impact our members and their constituents in the first responder community. As you requested, the focus of my testimony is on the impact of the Department of Homeland Security, Science and Technology Directorate (DHS S&T Directorate) on our nation's public safety communications. The issues that I have been asked to address are listed below. I want to emphasize that in addressing these issues I will be largely focusing on the communications and inter-operability issues, although I will also address the larger context of DHS support for the first responder community and localities.

- The role DHS should play in helping localities prepare for security threats and disasters.
- How well the FY 08 budget request for DHS S&T supports the development of technology for first-responders.
- DHS collaboration with State and local governments and the first responder community on standards development and how the first-responder community uses the results of DHS technology testing and evaluation and standards.
- The principal technological needs of the first-responder community.
- DHS' planning and priority-setting mechanisms and the communications needs of first responders.
- A reflection on the General Accounting Office Report of 2004 and the progress made to assist the first responders with inter-operability.

Protecting the public is a key responsibility of all levels of government. From federal agencies down to local fire protection districts the public depends on us. DHS plays a key role in this effort by supporting the 55,000 local public safety agencies in their daily challenges and during major disasters where it and other federal agencies provide direct response and service. DHS funding is a critical element that helps State and local public safety meet daily and catastrophic challenges. Communication is critical to meeting those challenges and DHS funding encourages all levels of responders to work together to promote better communications systems, including solving inter-operability and other public safety communications issues.

The National Incident Management System (NIMS)

DHS programs such as the National Incident Management System (NIMS) started out as a guide for major events, but local agencies now find that the NIMS structure is also effective during everyday events from fires to hostage situations. DHS supported the implementation of NIMS through the grant process and has been successful at encouraging local public safety to embrace and use NIMS during joint responses to emergencies. It is important to note that one of the reasons that NIMS works is because it was developed with input from the State and local practitioner community. As a result, DHS was able to both draw upon best practices from the people that do this work daily as well as obtain "buy-in'" for the final product.

DHS guidelines are now requiring local agencies to develop joint plans for multi-agency responses. Part of this challenge is that local agencies have long delayed sitting down and working together. With DHS funding directed at regional or cross jurisdictional responses, there is significant incentive to finally come together to share resources and manage incidents effectively.

Inter-operability

The heart of any coordination of an incident, large or small is communications. In this regard, the next round of federal grant dollars requires that states must develop statewide communications plans that also include counties, cities, and local districts. The guidelines for these statewide plans were developed by the SAFECOM Program located within the DHS Office of Inter-operability and Compatibility' (OIC), with the participation of local responders and public safety communications officials.

The significance of the national guidelines is they require prior planning and, at the same time, ensure that grant funds are spent on specific solutions in accordance with those plans. When the major issues are addressed at the local level, it also means they are addressed at the national level. The challenge is to ensure that the overall objectives meld into the State and local operational environment to enhance effective response.

Interagency communication problems have been identified in every major incident over the last 10 or more years. Solving this issue is not as easy as it might seem. State and local jurisdictions have invested billions of dollars in non-compatible communication systems that are operating in different bands of spectrum. The solution most often involves building new infrastructure which is very expensive. While the development of regional systems make sense, building them is also very expensive and requires a heightened level of cooperation among agencies. It also involves knowledge of best practices that is not always available at the local level. What has emerged is not only an emphasis on infrastructure and equipment, but the planning and cooperation needed to make use of these resources effectively across all agencies.

The DHS Office of Inter-operability and Compatibility's SAFECOM Program has been one of the true successes in providing assistance to State and local agencies to meet these challenges. SAFECOM provides research, development, testing and evaluation, guidance, tools, and templates on communications-related issues that improve emergency response through more effective and efficient inter-operable wireless communications.

The key to the success of SAFECOM is that it is a practitioner-driven program and has developed a process to facilitate the input of local and State emergency response practitioners. SAFECOM, working with its Executive Committee, the Emergency Response Council, and organizations in the practitioner community, like NPSTC, developed a national plan to enhance inter-operability, a Statement of Requirements for communications equipment, systems, and tools to assist jurisdictions to develop governance structures and planning; and, consequently, helped facilitate the quicker adoption of standards and grant guidance for communications-related grant programs, among other things.

Most recently SAFECOM completed a national Baseline Study of Inter-operability to learn what the problems were at the local level. DHS also developed a Scorecard of Inter-operability in designated Urban Areas (UAs) using public safety practitioners in the process. A key next step will be to develop a scorecard on standards compliance testing at the local level, something sorely needed to assist State and local jurisdictions in making the right procurements.

The "scorecard" reviews of the UAs focused on three main areas: Governance (leadership and strategic planning); Standard Operating Procedures (plans and procedures); and Usage (use of equipment). The evaluation criteria was derived directly from the SAFECOM Inter-operability Continuum and Inter-operability Maturity Assessment Model that depicts the key components of inter-operability—governance, standard operating procedures, usage, technology, and training and exercises.

The findings identify gaps and areas for improvement. Key findings included:

- Plans for inter-operable communications are now in place in all 75 urban and metropolitan areas, but implementation is now needed.
- Regular testing and exercises are needed to effectively link disparate systems and facilitate communications between multi-jurisdictional responders, including State and federal agencies.
- Cooperation among first responders in the field is strong, but formalized governance (leadership and strategic planning) across regions is not as advanced.

In my opinion, these are important findings and should apply to all areas of public safety nationwide, not just the Urban Areas.

There also needs to be an examination to determine the level of inter-operability in the non-urban areas of our nation. This will provide a better idea of where we stand and the basis for determining future costs. Since 2003, DHS has awarded $2.9 billion in funding to enhance State and local inter-operable communications efforts;

this is a small amount, given that experts estimate an $18 billion infrastructure nationwide that is not inter-operable and the equipment is outdated. We will continue to see an inter-operability improvements only if there is adequate funding and grant guidance to promote regional and statewide planning and systems.

Compliance Testing

Compliance testing of radio equipment is one item best done at the national level. Local agencies do not have the facilities, experience, or the type of equipment to do in-depth compliance testing. For example, at the present time there is only one national standard for radio equipment, commonly referred to as P25 and relating to inter-operability. While several manufacturers make claims that their products are P25 compliant; testing is necessary to validate their claims.

There is a need for a federal agency to perform these compliance tests and DHS SAFECOM, along with their partners at the National Institute of Standards and Technology (NIST) and the National Telecommunications and Information Agency (NTIA) Institute for Telecommunication Sciences (ITS) fill this role. This is especially true in that the Department of Defense (DOD), other federal departments and State and local agencies are now all using P25 radio equipment. There is no real magic in which agency does the testing; it just needs to be done.

The NIST Office of Law Enforcement Standards (OLES) technical staff has been involved with NPSTC for many years, and they have included our volunteers in the development and review of the SAFECOM Statement of Requirements (SOR) for public safety technology. They have worked closely with NPSTC as it develops consensus positions on the best technology use for first responders and provides a welcome check and balance to their work.

Broadband

An example of our collaboration occurred last month when NIST/OLES in Boulder, Colorado worked with NPSTC to develop user's needs in broadband. The effort expanded the input of 57 practitioners who had provided input into the needs study. With NPSTC support, 627 practitioners agreed to provide input to the project. Such collaboration is mutually beneficial to both the local and federal communities. The SAFECOM Program provides an important mechanism for this collaboration.

The focus on new and innovative technology today is in broadband for public safety. Ten years ago the public safety community could not have imagined that broadband technology would have advanced as it has today and have the potential to provide so much. The concern today is that broadband was not planned for nationwide use, and yet to ensure inter-operability that is what we need, a nationwide broadband network that is controlled by and built to public safety standards. The testimony to the Senate on February 8, 2007, of Chief Harlin McEwen representing the International Association of Chiefs of Police (IACP), the Association of Public Safety Communications Officials-International (APCO), the Major Cities Chiefs Association (MCC), the National Sheriff's Association (NSA), and the Major County Sheriff's Association and NPSTC along with the testimony of Chief Charles Warner representing the International Association Of Fire Chiefs (IAFC) regarding broadband for public safety is attached to this document. This testimony is supported by all of the major public safety associations and NPSTC.

The SAFECOM Inter-operability Baseline survey was sent to 22,400 randomly selected law enforcement, fire response and emergency medical services (EMS) agencies. Findings indicate that roughly two-thirds of emergency response agencies across the Nation use inter-operable communications in varying degrees. Agencies tend to be more developed in technology than they are in standard operating procedures and exercises. Cross-discipline and cross-jurisdiction inter-operability at the local level tends to be more advanced than between State and local agencies. In addition, law enforcement, fire response, and EMS agencies reported similar levels of development in most areas of inter-operability.

To date, no national survey has addressed broadband systems owned by public safety since there is currently little or no available (700 MHz or 4.9 GHz) spectrum for this use. The 700 MHz block of spectrum that will become available with the digital television transition will be the first opportunity for local public safety to use these new technologies. Many local agencies have developed and filed their plans with the FCC for local and regional use of the broadband spectrum. The transition and release of this spectrum to public safety remains critical.

SAFECOM, in conjunction with NIST/OLES, recently brought together key stakeholders from both industry and the public safety community to discuss and clarify the varying perceptions of Voice over Internet Protocol (VoIP's) role in public safety communications. This technology has the potential for significant impact on public safety communications. Yet there must be the ability to test its use for mission-crit-

ical activities and ensure its robust nature before marching into nationwide acceptance on local networks.

Funding Levels and Priorities

Of great concern to the public safety community is that despite the critical work being done by OIC's SAFECOM program, it has never been adequately funded. In Fiscal Year 2007 OIC's entire budget was $27.2 Million to fund SAFECOM and other programs of importance to the first responder community. The Inter-operable Communications Technical Assistance Program (ICTAP) run by the Grants and Training Office (G&T) only received $10 Million. The newly created Office of Emergency Communications (OEC) has received no funding to date. Given the critical nature and magnitude of the challenge, this is woefully inadequate. The expectation of other agencies transferring portions of their budgets to fund the DHS OEC is time consuming and creates concern among the other federal agencies. It has also caused confusion and uncertainty amongst the State and local community.

DHS needs to continue to more broadly encourage the development of regional systems that are multi-jurisdictional, multi-disciplined, and inter-operable for all responders. With over 55,000 public safety entities in this nation, each supporting their own systems and political jurisdiction, as I noted earlier, the estimate to upgrade and/or replace communications equipment is over $18 billion dollars.

For example, I come from Orange County (Orlando) Florida. Our county radio system cost $21 million in 1992 when it was built, and new sites continue to be added to accommodate growth, at a cost ranging from a quarter of a million to a million dollars per radio site. This is one system in one of Florida's 67 counties. Within Orange County, there are several small cities and the City of Orlando which maintain individual systems. I was with the City of Orlando where I retired after 27 years with the Police Department. During that time we built a $10 million dollar system while the county was building their $21 million dollar system. We pursued joining the County and building one system but were unable to cross the barriers to make that happen. This is common around the U.S. Incentives are needed to eliminate duplication and waste of taxpayer money.

NPSTC was formed for the sole purpose of bringing the multitude of public safety disciplines together to address communication issues. In this area we have found that DHS, primarily through SAFECOM, not only consults with our community on issues, but solicits our participation in helping them develop planning and priorities. It embraces the objective of making improvements in public safety communications with the important recognition that local and State participation is crucial. A cooperative working relationship has been established over the years and our community values the input and assistance that we receive not only from DHS, but from the several federal agencies that interrelate with us on a regular basis.

The success of homeland security depends in large part on the success of local public safety. Local public safety relies on the support and guidance it receives from its federal partners. The Department of Homeland Security should continue to facilitate a robust and substantive intersection between the Federal Government and the response community.

In addition to the Office of Inter-operability and Compatibility, we are currently working with the NIMS Integration Center and other offices to update the National Incident Management System and the National Response Plan. We also work with the Office of Grants and Training. The success of working together is critical to ensure that policies and procedures are operationally driven and able to be realistically implemented on the ground.

Areas that need continued enhancement of the federal-public safety relationship include critical infrastructure protection and information/intelligence sharing offices. There is evidence of movement in information and intelligence sharing, but the emergency services' role in critical infrastructure protection continues to be challenging—due, in part, to emergency services unique role as both protector of sectors and a sector to be protected.

A final note, and on a larger scale, intersections between local, State and federal entities cannot be identified nor trusting relationships built if the landscape and personnel are constantly changing. DHS's impending re-organization will prove another test—but also an opportunity—to form relationships between the Federal Government and first responders.

The 2004 General Accountability Office Report

In September 2004, the GAO released a report on inter-operability and testified before the Subcommittees on technology, Information Policy, Intergovernmental relations, and Census, House of Representatives titled *Federal Leadership Needed to Facilitate Inter-operable Communications Among First Responders*

Set forth below is what the GAO determined and our view of the progress three years later:

GAO: (1) In a recent report on inter-operable communications, we recommended that the Secretary of DHS (1) continue to develop a nationwide database and common terminology for public safety inter-operability communications channels.

Progress to date: With the support of the SAFECOM Program, NPSTC recently completed a forum and methodology for responders to work toward common nomenclature. NPSTC has made progress and has a consensus on several key issues. A report has been distributed for review and comment, and we will be making a final recommendation to our Governing Board in June 2007. Federal support and adoption by the FCC is now needed to formalize the use of common channel naming across the Nation.

GAO: (2) help states assess inter-operability in specific locations against defined requirements.

Progress to date: Through DHS Grants and Training grant awards, 75 Urban Area Security Initiative (UASI) locations began developing plans and were accessed by a standardized scorecard developed by SAFECOM and member associations. This is important progress and must be extended statewide beginning in 2007.

GAO: (3) through federal grant awards, encourage State action to establish, and support a statewide body to develop and implement detailed improvement plans.

Progress to date: The SAFECOM Program created grant criteria, which were placed in the DHS Grants; however it has taken until March 2007 for the first national meeting hosted by the National Governors Association (NGA), SAFECOM, and NPSTC to begin statewide planning. This process will request states to voluntarily provide an "inter-operability coordinator" statewide and provide guidance for states to begin developing statewide plans.

GAO: (4) require that grant applications be in compliance with statewide inter-operability plans, once they are developed.

Progress to date: Several states have made good progress to complete their plans, however many are just beginning. The Grant guidance prepared by SAFECOM, supports this recommendation.

GAO: GAO also recommended that the Director of OMB work with DHS to review SAFECOM's functions and establish a long-term program with appropriate authority and funding to coordinate inter-operability efforts across the Federal Government.

Progress to date: In the opinion of the public safety community which I represent, the SAFECOM Program has never been funded at an appropriate level. The fluctuation in budgeted funds belies any attempt for long-term programs to be successful. Short quick fixes become the norm and the possibility for a long-term strategic plan that stays the course until it is completed is threatened when funding fluctuates in these extremes. In addition to the tools and critical studies (Baseline Study, etc.), SAFECOM also tests and evaluates technologies, conducts pilot programs, and funds the standards compliance testing. None of these efforts have adequate resources.

GAO: The current wireless inter-operable communications capabilities of first responders nationwide have not been determined. To assess these capabilities, a set of requirements is needed that can be used to assess "what is" compared to "what should be." The Office of Management Budget (OMB) has established the Wireless Public Safety Inter-operable Communications Program, SAFECOM, within the Department of Homeland Security (DHS) as the focal point for coordinating federal efforts to improve inter-operable communication.

In April 2004, SAFECOM issued a document designed to serve as a set of baseline requirements and is working to develop a baseline of current capabilities by July 2005.

Progress to date: The baseline was published in 2006 and UASI scorecards were published in 2007.

GAO: The Federal Government can take a leadership role and provide support for developing:

(1) a national database of inter-operable communication frequencies,

Progress to date: This remains a challenge, the closest version is the 700 MHz "notebook of frequencies" developed by NPSTC and funded and maintained by the National Institute of Justice (NIJ).

GAO: (2) a common nomenclature for those frequencies,

Progress to date: NPSTC continues to commit significant work on this issue. SAFECOM has included a grant guidance principle to encourage common channel naming.

GAO: (3) a national architecture that identifies communications requirements and technical standards,

Progress to date: This is an in-progress task undertaken by the SAFECOM Program. This is a very technical and expensive process that does not have adequate resources at this time.

GAO: (4) statewide inter-operable communications plans.

Progress to date: This process began in 2007.

GAO: State and local governments can play a large role in developing and implementing plans to improve public safety agencies' inter-operable communications. State and local governments own most of the physical infrastructure of public safety communications systems, and states play a central role in managing emergency communications. States, with broad input from local governments, are a logical choice to serve as a foundation for inter-operability planning because incidents of any level of severity originate at the local level with states as the primary source of support.

However, states are not required to develop inter-operability plans,

Progress to date: States are not required to develop inter-operability plans; however States must have a plan to qualify for federal communications grant funds.

GAO: there is no clear guidance on what should be included in such plans.

Progress to date: SAFECOM is proving planning guidance to the states at the March 2007 meeting and funding is being made available to support the development of statewide planning assistance.

It is NPSTC's view that the DHS SAFECOM Program has worked diligently to meet the goals identified in the GAO report and has provided support to the local communities, recognizing that it must be a practitioner-driven program. SAFECOM has achieved inter-operable communications at the command level, defined as communications within one hour of a major event, in the 10 highest threat urban areas, as part of its Rapid COM 1 initiative. It has published a step-by-step planning guide for developing a locally driven statewide strategic plan for inter-operable communications and facilitated regional communications inter-operability pilots that assist local officials in the implementation of their statewide plans.

In addition to the practitioner input SAFECOM seeks from NPSTC and the practitioner community, SAFECOM seeks advice from the first responder community through its Executive Committee (EC) and the Emergency Response Council (ERC). The SAFECOM EC is comprised of representatives from local and State emergency response agencies and professional associations, as well as contributing federal agencies. Working through the associations is critically important to ensure State and local collaboration with the Federal Government. The EC serves as the primary steering group for the SAFECOM Program. Montgomery County, Maryland, Council chairwoman Marilyn Praisner, National Association of Counties (NACo), serves as EC Chair, and Mr. Glen Nash, Past-President, Association of Public-Safety Communications Officials, International (APCO), serves as Vice Chair.

Representatives from the following organizations also serve on the EC:

- Association of Public Safety Communications Officials—International, Inc. (APCO)
- Department of Homeland Security (DHS) Chief Information Officer (CIO)
- Department of Justice (DOJ) Chief Information Officer (CIO)
- International Association of Chiefs of Police (IACP)
- International Association of Fire Chiefs (IAFC)
- Major Cities Chiefs Association (MCC)
- Major County Sheriffs' Association (MCSA)
- National Association of Counties (NACo)
- National Association of State EMS Directors (NASEMSD)
- National Governors Association (NGA)
- National Institute of Justice Communications Technologies (NIJ CommTech)
- National Institute of Standards and Technology (NIST)
- National League of Cities (NLC)
- National Public Safety Telecommunications Council (NPSTC)

- National Sheriffs' Association (NSA)
- Office of Management and Budget (OMB)
- U.S. Conference of Mayors (USCM)

The SAFECOM ERC provides a mechanism for individuals with specialized skills and common interests to share best practices and lessons learned so that interested parties at all levels of government can learn from one another's experience, perspective, and expertise. Its membership, which comprises representatives from the local, tribal, State, and federal emergency response and policy-maker communities, is a key resource for the improvement of emergency response communications inter-operability.

Representatives from the following organizations serve on the ERC:

- American Association of State Highway and Transportation Officials (AASHTO)
- American Public Transportation Association (APTA)
- Automated Regional Justice Information System (ARJIS)
- Capital Wireless Integrated Network (CapWIN)
- Community Oriented Policing Services (COPS)
- Council of State Governments (CSG)
- Department of Agriculture (DOA)
- Department of Commerce (DOC)
- Department of Defense (DOD)
- Department of Energy (DOE)
- Department of Interior (DOI)
- Department of Health and Human Services (HHS)
- Environmental Protection Agency (EPA)
- Federal Communications Commission (FCC)
- Federal Emergency Management Agency (FEMA)
- Federal Partnership for Inter-operable Communications (FPIC)
- InterAgency Board (IAB)
- International Association of Emergency Managers (IAEM)
- International City/County Management Association (ICMA)
- International Municipal Signal Association (IMSA)
- Joint Tactical Radio System (JTRS)
- National Aeronautics and Space Administration (NASA)
- National Association of Regional Councils (NARC)
- National Association of State Chief Information Officers (NASCIO)
- National Association of State Telecommunications Directors (NASTD)
- National Association of State EMS Directors (NASEMSD)
- National Association of Telecommunications Officers and Advisors (NATOA)
- National Criminal Justice Association (NCJA)
- National Emergency Management Association (NEMA)
- National Emergency Number Association (NENA)
- National Guard Bureau (NGB)
- National Institute of Standards and Technology (NIST)
- National Native American Law Enforcement Association (NNALEA)
- National Public Safety Telecommunications Council (NPSTC)
- National Telecommunications and Information Administration (NTIA)
- Office of Domestic Preparedness (ODP)
- Office of Management and Budget (OMB)
- SEARCH
- Telecommunications Industry Association (TIA)
- USDA Forest Service

Summary

The work of the Department of Homeland Security in public safety communications is vital if we are to meet the expanded demands of domestic security and

emergency response. We believe that DHS, its SAFECOM program and other component agencies diligently pursue this responsibility and recognize the critical importance of meaningful local participation.

In closing, I think there are two issues the Subcommittee should consider as part of the overall effort to improve public safety communications. First, the fluctuation in funding of the budget as it pertains to communications inter-operability deters progress. A more stable environment with a better estimate of funding levels for a three- to five-year period would allow the planning and funding participation to be pursued. The result would be more participation and system improvements.

The second issue is a proposal to permit the creation of a Public Safety Broadband Trust in 700 MHz and reallocating 30 MHz of spectrum scheduled to be auctioned. This broadband trust would be a first for public safety. With a Congressional embrace, a nationwide broadband inter-operable radio system could be built that would permit first responders to have everything from blackberry type messages to full motion video of incidents. It would be paid for by private funds as the system would sell excess capacity to non-public safety users. It is also a way to bring the advantages of broadband to rural areas that now have none. It would expand access to new technologies without burdening taxpayers. We urge members to examine this issue very closely; it would make a positive and important contribution to public safety communications.

Thank you again for the invitation to appear before the Subcommittee. I would be pleased to respond to any questions.

WRITTEN TESTIMONY OF
HARLIN R. MCEWEN
CHAIRMAN, COMMUNICATIONS & TECHNOLOGY COMMITTEE
INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE (IACP)

COMMUNICATIONS ADVISOR
MAJOR CITIES CHIEFS ASSOCIATION (MCC)
NATIONAL SHERIFFS' ASSOCIATION (NSA)
MAJOR COUNTY SHERIFFS' ASSOCIATION (MCSA)

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE & TRANSPORTATION
UNITED STATES SENATE

FEBRUARY 8, 2007

CURRENT AND FUTURE PUBLIC SAFETY COMMUNICATIONS

Thank you, Mr. Chairman, and distinguished Members of the Committee for the opportunity to appear before you today.

My name is Harlin McEwen and I have been actively involved in public safety for almost 50 years. My career has been in law enforcement and I also have been a volunteer firefighter. I am the retired Police Chief of the City of Ithaca, New York, and am also retired as a Deputy Assistant Director of the Federal Bureau of Investigation in Washington, DC. I serve as Chairman of the Communications and Technology Committee of the International Association of Chiefs of Police (IACP), a position I have held for more than 28 years. I also serve as the Communications Advisor for the Major Cities Chiefs Association (MCC), the National Sheriffs' Association (NSA), and the Major County Sheriffs' Association. I am the Vice Chairman of the National Public Safety Telecommunications Council (NPSTC) and am a Life Member of the Association of Public-Safety Communications Officials-International (APCO). Today I speak on behalf of all of these organizations.

When I first became a law enforcement officer in 1957 police vehicles had tube type six volt analog mobile radios that dimmed the headlights when we pushed the microphone button. In those days there were no hand held radios. In my career I have witnessed many changes and advances in law enforcement and public safety communications. However, the advances for public safety have consistently lagged behind the advances of commercial services, primarily because of lack of funding and spectrum.

As you are aware, citizens rely upon their local and State police agencies, sheriffs' offices, fire departments, emergency medical services, and other emergency services like highway and public works and utilities to come to their assistance wherever and whenever needed. They respond whether it is a crime in progress, a civil disturbance, a building fire, a forest fire, an automobile accident, a health emergency, a natural disaster, or, as we learned on 9/11, a terrorist attack. Today, citizens assume that those first responders will get the call and will have the communications tools they need to address emergencies quickly and efficiently. Unfortunately that is not always true.

I want to applaud the efforts of this committee and the Congress in voting to clear the television broadcasters from the long promised 700 MHz spectrum. This will help us improve public safety radio communications, both operability and inter-operability. The major cities and metropolitan areas of this country are still in desperate need of additional land mobile voice channels and are anxiously waiting for this spectrum to become available. Your efforts to designate $1 billion derived from the auction of radio spectrum for public safety communications are also very much appreciated by the public safety community and will be very helpful. The introduction of S.385 by Senators Inouye, Stevens, Kerry, Smith, and Snowe is also helpful in giving direction to NTIA with respect to the $1 billion grant program and we appreciate these efforts to have this funding program implemented in a timely fashion.

I am pleased to have the chance to discuss with this committee an exciting new opportunity for Congress to take steps that will pave the way to reducing the dependence on local and federal tax revenues to maintain modern public safety communications systems. That is a proposal for a 700 MHz nationwide public safety

broadband network. This proposed network can become a reality only if Congress authorizes creation of a public/private partnership, controlled by the public safety community, to hold a nationwide license for 30 MHz of spectrum in the upper 700 MHz band and further authorize us to deploy this network pursuant to a public sector-private sector partnership model.

I have studied the issue of public safety telecommunications for decades. I have been actively engaged in the efforts of the Federal Communications Commission, other federal agencies, State and local government entities and individual departments to identify law enforcement communications requirements and provide our first responders with the necessary tools to meet those needs. Substantial time and significant taxpayer dollars have been devoted to those efforts, yet in 2007 the public safety community still is far behind commercial users in terms of wireless functionality. Our public safety users who should have the best, most advanced, and most robust capabilities too often must rely on systems that are inadequate for their needs today, much less the expanded responsibilities with which they will continue to be charged in the future. Without a fundamental change in the way we approach emergency responder communications, specifically without allocation of the additional 30 MHz of spectrum and adoption of the approach embodied in the Public Safety Broadband Trust (PSBT) proposal, I see no reason to ever expect substantial improvement.

The wireless voice systems public safety personnel use today are among the most important tools they have to do their job in a safe and efficient manner. However, these systems have in many cases been under funded, poorly maintained and generally not refreshed. As we look to the long-term future, we need to look at new and better ways to improve public safety communications.

The need for more efficient public safety data systems is growing and this has become the focus of much of our attention as we look to ways for public safety to take advantage of Third Generation (3G) and Fourth Generation (4G) technologies.

The implementation of a nationwide public safety broadband network can also be the beginning of the end to the problem of public safety inter-operability. We have been asking for funding support for years to help us upgrade and replace mission critical land mobile voice systems that are built by different manufacturers, are of different vintages, and are generally incompatible and in many cases not compatible with the P25 standards, the only recognized national digital standards for land mobile public safety communications inter-operability.

It is critical to understand that this is a one time only opportunity to solve many of the public safety communications requirements of today and the future. We recognize this is not an easy decision for the Congress. You must choose between solving the public safety communications problem and making sure our citizens have good public services, or allowing the spectrum required by public safety to be auctioned to commercial companies who want to expand their services and increase their profits. It seems simple to us that by your approval of this important step for public safety you will be doing the right thing for America. It will begin to take the burden off the taxpayers who must build and maintain increasingly expensive public safety communications systems.

The benefits from a nationwide public safety broadband network as set forth in the Public Safety Broadband Trust proposal are as follows:

1. Broadband data services (such as text messaging, photos, diagrams, and streaming video) not currently available in existing public safety land mobile systems.
2. A hardened public safety network with infrastructure built to withstand local natural hazards (tornadoes, hurricanes, earthquakes, floods, etc) that would include strengthened towers and back up power with fuel supplies to withstand long-term outages of public power sources.
3. Nationwide roaming and inter-operability for local, State, and federal public safety agencies (police, fire and EMS) and other emergency services such as transportation, health care, and utilities.
4. Access to the Public Switched Telephone Network (PSTN) similar to current commercial cellular services.
5. Push to talk, one to one and one to many radio capability that would provide a backup to (but not replace) traditional public safety land mobile mission critical voice systems.
6. Access to satellite services to provide reliable nationwide communications where terrestrial services either do not exist or are temporarily out of service.

For those who argue that public safety already has enough radio spectrum to meet current and projected mobile requirements, I can only say that they purposely ignore the facts concerning public safety spectrum allocations and first responder communications requirements. As an example, the cellular industry, represented by CTIA, has grossly misrepresented the spectrum issue as recently exhibited in their press release critical of Senator McCain's announcement that he would be introducing legislation to establish a new nationwide, state-of-the-art public safety broadband network. The CTIA statement said "the basic facts of the matter should compel this important debate to be about providing first responders with funding, access to equipment and coordination, not more spectrum." CTIA further stated "Right now, the public service community utilizes 47 MHz of spectrum to serve its public safety users. At the same time, there are wireless carriers that use roughly the same amount of spectrum to deliver voice, data and advanced information services to many times that number of subscribers. More spectrum is clearly not the answer."

Contrary to what the CTIA says, the REAL facts on spectrum allocations are as follows:

STATE AND LOCAL PUBLIC SAFETY SPECTRUM ALLOCATIONS

Allocation	MHz
VHF Low Band (25-50 MHz)	6.3
VHF High Band (150-174 MHz)	3.6
UHF Low Band (450-470 MHz)	3.7
800 MHz Band (806-821/851-866 MHz)	3.5
800 MHz Band (821-824/866-869 MHz)	6.0
700 MHz Band (764-776/794-806 MHz)	24.0
TOTAL PUBLIC SAFETY	**47.1**

COMMERCIAL SPECTRUM ALLOCATIONS

Allocation	MHz
Cellular	50
Broadband PCS	120
AWS	90
Broadband Radio Services	190
Lower 700	48
Upper 700	30
TOTAL COMMERCIAL	**528**

But even these numbers do not tell the real story or explain why existing public safety allocations cannot be used for broadband operations. Historically, the FCC has allocated individual channels, not contiguous channel blocks, for public safety use. These channels are immediately adjacent to channels allocated for taxicab companies, truck operators and other businesses. The channels typically are no larger than 25 kHz bandwidth and more frequently 12.5 kHz, or a tiny fraction of each 25 MHz cellular system authorization. This allocation approach has permitted numerous governmental entities to secure licenses for localized, individual purposes, but precludes the public safety community as a whole from consolidating enough contiguous channels to deploy 21st century broadband technology networks. There simply is not sufficient contiguous bandwidth to support the text messaging, building diagrams, photos, streaming video and other transmissions that will be as essential to law enforcement officers during these perilous times as the weapons they carry.

While the 24 MHz public safety allocation in the upper 700 MHz band is contiguous, even that spectrum is subdivided in various categories designed for mission critical voice communications on both localized and State levels, as well as for wideband data applications. And that spectrum allocation, first promised to the public safety community in 1997, was intended to address the unmet needs and identified deficiencies in the spectrum resources available to public safety more than a decade ago. New technologies and new services have since been developed to respond to the ever escalating commercial appetite for more useful and sophisticated mobile communications tools and solutions—and appropriate new commercial spectrum allocations have been made available to commercial network operators to bring those improvements to their customers. Likewise, over the past decade, public safety's needs for access to these advanced technologies, services, tools and solutions has not stood still—although, unfortunately, the amount of appropriate spectrum allocated to meet them has.

Allow me to emphasize these points by example, as the contrast between the spectrum resources available to commercial wireless network operators and to the public safety community could not be more striking. To begin with, commercial cellular and PCS licensees have access to large blocks of contiguous spectrum. Their allocations were specifically designed to support system architectures and technologies that would accommodate vast numbers of customers. To compare the number of subscribers that can be served on a 25 MHz cellular network with the number of police

officers that can share a 12.5 kHz bandwidth channel, or even multiple channels, is as meaningful as comparing the size of watermelons to grapes. Compounding the imbalance is the absolute amount of spectrum that has been made available for commercial use in comparison to that which has been made available for public safety uses as detailed above. Just last year, the Commission made another 90 MHz of spectrum of Advanced Wireless Spectrum available for commercial operations, again in large spectrum blocks and expressly authorized for commercial mobile broadband uses.

In fact, it is the success of the cellular/PCS model that has convinced us that public safety must have a 30 MHz spectrum block on which to deploy an advanced technology broadband network. That model has persuaded us that the public safety community must join together in the Public Safety Broadband Trust, rather than seeking individual licenses for individually designed and deployed systems, if we are to achieve our objective: seamless nationwide roaming capability on a 21st century broadband 700 MHz network that is built and operated to satisfy increasing and demanding public safety requirements.

I stated previously that a nationwide broadband network solution needed to address both spectrum and funding, and to address them both at the same time and in the same context. The latter is just as critical as the former and requires an innovative approach given the extraordinary costs associated with building and operating a truly nationwide broadband network. Unlike purely commercial systems that have the luxury of limiting coverage to areas of denser population and transportation corridors, public safety users must have communications capability wherever there are people or property to protect. This mandate has the important consumer benefit of ensuring that a broadband network designed to meet public safety needs will be available in suburban and rural communities that remain outside the areas of commercial broadband deployment. However, I have substantial experience in the traditional funding sources for public safety communications and see no realistic possibility that the necessary monies will be made available even to build, much less maintain, operate and routinely upgrade a network of this scope if dedicated to purely public safety requirements.

The only solution that we consider viable is a public sector-private sector partnership as proposed in the Public Safety Broadband Trust. Under this approach, the PSBT would acquire a 30 MHz license at 700 MHz and would enter into leases of spectrum usage rights with commercial operators who would build a nationwide public safety network that (1) would be paid for by commercial operators using excess capacity, not by the public safety community or the taxpayer; (2) would be licensed and controlled by public safety representatives to ensure public safety priority access; and (3) would be refreshed with the latest technical improvements, funded by the commercial participants.

We do not support what some would call a "hosted" public safety network. While the term may have somewhat different meanings to different people, at its core it puts mission critical, emergency response communications in a position of dependence with respect to the host commercial provider. Moreover, it undermines or even negates the essential nationwide character of the network. With all due respect to commercial operators that might now express support for hosted systems, there is nothing in the over 20-year history of commercial wireless systems that would validate their reliability or availability for mission critical public safety needs. That is not an arrangement that the public safety community could endorse.

In regard to the 9th Notice of Proposed Rulemaking (NPRM) recently issued by the Federal Communications Commission, we have many concerns about the concepts set forth in that proposal. The 9th NPRM suggests that a nationwide broadband network could be built using the 12 MHz of spectrum currently allocated for local licensing of public safety wideband systems. This would take away from local licensing control the spectrum long promised for use by local agencies. In addition we believe the proposal is seriously flawed by failing to acknowledge the need for enough spectrum to attract investors to participate in a public/private partnership where private funds would be invested to build a nationwide network.

By contrast, the partnership outlined in the Public Safety Broadband Trust creates a symbiotic and balanced relationship, but one in which public safety always remains in control. It represents a win-win opportunity if sufficient spectrum is allocated to accommodate both public safety and commercial usage. Public safety cannot fund this network on its own, but also must be confident that the network is built to hardened public safety requirements with priority access that is adequate to respond to emergencies. Commercial operators will lease the spectrum and build the network to public safety specifications, but only if there is sufficient excess capacity to permit meaningful commercial service on a regular basis. The technical data sup-

ports the conclusion that a minimum of 30 MHz is needed to serve these complementary requirements.

The many public safety organizations and agencies that have supported the PSBT approach recognize that it will require removing some of the 700 MHz spectrum that currently is scheduled to be auctioned. The PSBT proposal includes a plan to make the federal budget whole. The PSBT would raise $5 billion to pay the U.S. Treasury for the spectrum, using the revenues from the commercial users and the assistance of federal loan guarantees similar to those that have been made available to industries such as airlines, pipelines and automobile manufacturers. This financing arrangement would ensure that other federal public safety spending priorities, including the $1 billion for other public safety inter-operable communications needs, would not be affected.

Let me add that I and other supporters of the PSBT also endorse the commendable work being done by local and regional organizations such as the Capitol Area Region Broadband Project with respect to broadband. To the extent their efforts bring about public safety communications improvements, it is important work that deserves support. But we must remain mindful that the results will be, at best, a patchwork of improved, but incompatible, non-inter-operable networks at a daunting per unit cost. They are doing what they can in light of the regulatory and financial environment in which they must operate, but this nation can and must do better.

I have dedicated most of my professional career to the advancement of public safety communications. From that perspective, I believe this Congress has an extraordinary time sensitive opportunity. Approval of the PSBT and the public sector-private sector partnership will catapult public safety to its rightful place in the forefront of communications capability while at the same time delivering broadband service to communities that continue to be bypassed by the commercial telecommunications revolution. I hope you will share my belief that this is an opportunity that must be seized for the benefit of the entire American public.

Public Safety Broadband Trust

STATEMENT BY FIRE CHIEF CHARLES L. WERNER
INTERNATIONAL ASSOCIATION OF FIRE CHIEFS

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE & TRANSPORTATION

UNITED STATES SENATE

FEBRUARY 8, 2007

Good morning Mr. Chairman and Members of the Committee. I am Charles Werner, Fire Chief of the Charlottesville Fire Department in Virginia and a member of the Communications Committee of the International Association of Fire Chiefs IAFC). I am appearing today as the representative of the International Association of Fire Chiefs whose 12,000 members represent the leadership of America's fire and rescue service from small, rural, volunteer fire departments to the large, urban, metropolitan fire departments. Last year America's fire service responded to over 23 million fire and emergency calls covering incidents of structure fires, wildland/urban interface fires, emergency medical situations, hazardous materials incidents, technical rescues, and natural disasters. We are prepared, as well, to respond to the aftermath of terrorist attacks. I appear today to address a specific and growing communications need for America's fire service—broadband technology. Our testimony also reflects the views of the Association of Public-Safety Officials International, Inc.

PUBLIC SAFETY SPECTRUM NEEDS

At the request of Congress, the National Telecommunications and Information Administration (NTIA) and the Federal Communications Commission (FCC) established the Public Safety Wireless Advisory Committee (PSWAC) to define and document the critical need for communications resources and the spectrum to support public safety through the year 2010. The final report was released on September 11, 1996. Three key problem areas were identified in the report:

> First, radio frequencies allocated to public safety had become highly congested in many, especially urban, areas. Usable spectrum for mobile operations is limited making it difficult to meet existing requirements much less to plan for future, more advanced communications needs.
>
> Second, the ability of agencies within and between jurisdictions to communicate with one another is limited. Yet inter-operability is desirable for success in day-to-day operations as well as larger scale operations in dealing with both man-made and natural disasters.
>
> Third, public safety agencies lack the spectrum to implement advanced communications features. A wide variety of technologies—both existing and under development—hold substantial promise to reduce danger to public safety and achieve greater efficiencies in the performance of their duties. Specifically mentioned in the 1996 report were broadband data systems, video systems for better capabilities including use of robotics in toxic and hazardous environments, and better monitoring and tracking of both personnel and equipment.

To implement the requirements identified, the advisory committee determined that more spectrum was required, as follows:

> Immediately, 2.5 MHz of spectrum for inter-operability from new or existing allocations.
>
> Within five years approximately 25 MHz of new public safety allocations are needed. The report suggested using spectrum from television broadcast channels 60–69 as soon as possible.
>
> Over the next 15 years (e.g., through 2011) as much as an additional 70 MHz will be required to satisfy the mobile communications needs of public safety.

These were the needs and recommendations addressed in the PSWAC report of 1996. Then, in December 2005 the FCC sent a Report to Congress On the Study to Assess Short-Term and Long-Term Needs for Allocations of Additional Portions

of the Electromagnetic Spectrum for Federal, State and Local Emergency Response Providers. This report was submitted pursuant to P.L. 108–458, the *Intelligence Reform and Terrorism Prevention Act of 2004.* In its conclusion, the FCC stated: "First, as to the operation and administration of a potential nationwide inter-operable broadband mobile communications network based upon input from federal, State, local and regional emergency response providers, emergency response providers would benefit from the development of an integrated, inter-operable nationwide network capable of delivering broadband services throughout the country. Second, as to the use of commercial wireless technologies, while commercial wireless technologies and services are not appropriate for every type of public safety communication, there may now be a place for commercial providers to assist public safety in securing and protecting the homeland."

For the above stated reasons, the National Public Safety Telecommunications Council [a resource and advocate for public safety organizations in the United States on matters relating to public safety telecommunications] has filed comments with the FCC in support of reallocating 30 MHz of spectrum in the upper 700 MHz band, currently slated for auction, to create a public/private nationwide broadband network to be managed by public safety for the benefit of public safety. The filing states: "In an era where government preparedness is crucial, there is no nationwide public safety network to manage and coordinate response. There is no wide scale broadband technology capability to expedite analysis and information sharing critical to emergency assistance, investigation and apprehension. Not only is the current public safety spectrum so congested as to constrain voice—much less permit broadband use for video and data, limited funding hinders the incremental improvements that can be made and which are only pursued on a system by system basis. That which is possible in communications today and what public safety agencies have available reflects an enormous divide. The result is tangible: slowed and hindered response across all services which puts lives at risk and property in danger.

"Although legacy systems will continue to play an important role in public safety communications, the opportunity presented by the yet to be auctioned 700 MHz channels is emphatic. Without this additional spectrum, there can be no national public safety network connecting all agencies. Using broadband technologies to transmit information across agencies and miles immediately will be the exception. Public safety communications will come up short in meeting its challenges."

The IAFC is a member of the governing board of NPSTC and an active participant in all of its proceedings. The IAFC fully concurs with the statements of support by NPSTC for the establishment of a nation-wide, public/private, broadband network that will harness the innovative power of the private sector but be managed by public safety for the benefit of public safety.

PUBLIC SAFETY BROADBAND REQUIREMENTS

In 1997, Congress addressed part of the issue of additional spectrum by directing the FCC to allocate 24 MHz in the upper 700 MHz band for use by public safety. As a result of the *Deficit Reduction Act* (P.L. 109–171), which passed last year at this time, this spectrum will finally become available for our use in February 2009. As was originally intended, it is to provide, for individual licensees, 12 MHz of voice channels and 12 MHz of wideband data channels. Fire and police departments are now in the planning process of building communications systems utilizing this new spectrum. Broadband capability for public safety, identified in the 1996 PSWAC report, is a vital and growing need for fire and police agencies. It is the next step following the allocation and implementation of the 24 MHz designed to alleviate current spectrum congestion and provide inter-operability. To meet the broadband need for public safety, the following requirements are established:

A nationwide, broadband network covering 99 percent of the population, 65 percent of the land mass, most of the critical infrastructure, and a network that supports urban, suburban and rural communities.

A network large enough to draw commercial support which is requisite for a nationwide network to be affordable for public safety.

A network built using next generation technology.

A network built to public safety ruggedness specifications to ensure reliability under severely adverse conditions.

A network governed by public safety.

A network which ensures priority access for public safety.

PUBLIC SAFETY USES OF NATIONWIDE BROADBAND NETWORK

The Public Safety Broadband Trust proposal provides public safety with enormous potential that does not currently exist.

A hardened public safety network would make possible nationwide roaming and inter-operability for public safety agencies at the federal (e.g., U.S. Coast Guard), State (e.g., highway patrol), and local (e.g., police, fire/EMS) levels. It would give public safety access to satellite services where terrestrial services either do not exist or are temporarily out of service. The network build-out would give rural areas—for the first time—broadband coverage and provided public safety there a communications tool that would be virtually impossible because of cost under any other scenario. In addition, this new network will protect nuclear power plants, dams, railroads and pipelines and other parts of the Nation's critical infrastructure in rural areas.

There are a number of technologies that are available today that fire departments would use—more will be developed, especially if an affordable broadband network is available. Some examples are:

Transmitting video, photographs, blueprints and other information both to and from an incident command post.

Advanced paging systems particularly useful for summoning volunteer firefighters/medics.

Mesh enabled architecture (MEA) for non-GPS broadband location system.

Fireground accountability systems—biometrics as well as location.

Smart building downloads enroute to an alarm.

Enhanced GIS mapping capability for building locations, critical infrastructure, target hazards, water systems, transportation systems, etc.

Personal Area Networks linking a portable radio carried by a firefighter to many useful and lifesaving accessories including a helmet video camera, video viewing device, health monitor, wireless self contained breathing apparatus (SCBA) microphone and speaker, or a handheld computer.

Vehicular Area Networks that could link a vehicle's radio to laptop computers, printers, remote headsets, bar code readers, and cameras.

Medical video and high-resolution image transmissions from the scene of an incident to the emergency department of a hospital where physicians can assess patient status and give on-scene and enroute treatment instructions.

PDAs for fire department leaders or for all firefighters.

A ONE–TIME OPPORTUNITY TO DO THE RIGHT THING

Senator McCain has announced his intension to introduced legislation to establish a Public Safety Broadband Trust. The trust will be composed of public safety organizations to hold a single license for 30 MHz of broadband spectrum to create a nationwide, public/private broadband network. The trust also will be the management group to oversee the policies, procedures and practices of the network. In other words, the public safety trust will run the network for the benefit of public safety.

The 30 MHz of spectrum that is being considered is immediately adjacent to the 24 MHz of spectrum allocated to public safety in 1997 and which will be available in 2009. This has considerable advantage over any other spectrum since radio communication devices can be dual purpose with the spectrum so close. This spectrum in the upper 700 MHz is also near existing public safety which is being relocated in the lower 800 MHz band.

This 30 MHz of spectrum is currently slated for auction. The *Deficit Reduction Act of 2005* requires the FCC to auction this spectrum by January 2008. Without legislation taking this out of the auction and allocating it for the public safety trust, this one-time opportunity will be lost forever.

CALL FOR ACTION

The Congress of the United States has a one-time opportunity, in the near-term, to provide public safety with a nationwide, broadband network. In order to be affordable for public safety, the network would have to have viable commercial capacity of about 30 MHz of spectrum. The network would be built to public safety ruggedness specifications. A Public Safety Broadband Trust would be created to hold the single license from the FCC for the 30 MHz of spectrum and would oversee management of the network. While the network volume would be largely commercial, public safety agencies would use what it needed with a built-in priority status. Com-

mercial use also ensures that sufficient capital will be available for maintaining the system and upgrading and refreshing newer technologies when they come along.

We urge the members of this committee to take the first action to create this Public Safety Broadband Trust by promptly reporting legislation to take 30 MHz from the pending auction and direct the FCC to reallocate it to public safety. We cannot suggest too strongly the urgent and identified need for broadband capability that public safety can use with assurance that it will work when needed, be available when needed, and is affordable. With a global war on terrorism being fought daily and homeland security interest at an all-time high, public safety, in defense of the homeland, should be operating on 21st Century technology. Thank you for the opportunity to address the committee. We appreciate your consideration of this most important public safety issue.

BIOGRAPHY FOR MARILYN WARD

Ms. Ward brings 35 years of experience as both an advocate for public safety telecommunications issues and as an administrator in public safety telecommunications, from her position as Manager of Communications at the City of Orlando and part-time police officer in her early days in public safety, to her role as Orange County Public Safety Communications Manager, from which she retired in 2005.

Ms. Ward has been involved with communications issues on every level-local, State and federal. A former president of the Association of Public Safety Communications Officials—International (APCO) and founding NPSTC Chair, Ms. Ward has served in many leadership roles such as:

APCO Task Force Leader on the Public Safety Wireless Advisory Committee (PSWAC)

Steering Committee Member of the National Coordination Committee (NCC)

Statewide Coordinator of the Regional Domestic Security Task Force Communications Committee Chairs in Florida

Florida Statewide Executive Inter-operability and Technology Committee

Ms. Ward holds a degree in Business and Management and has received many public safety-related awards in her career.

DISCUSSION

Chairman WU. Thank you very much, Ms. Ward. We open the first round of questions, and the Chair recognizes himself for five minutes.

Under Secretary Cohen, I understand that you all in the S&T Directorate are working on a strategic plan, and I would like to ask you about the status of the development of this strategic plan and the extent to which a formal risk assessment will play a role in your strategic planning.

Mr. COHEN. Yes, sir, Mr. Chairman. As I have previously testified this year to the Homeland Security Committee, I owe the Congress two strategic plans. One is for the directorate itself, and that will be risk informed and customer focused. And some of the other panel members here have already discussed the importance of that. I have committed to the Congress that you will have that by June of this year.

The second that I owe was mandated by the enabling legislation. This is a much broader strategic plan, and it recognizes the wisdom of the enabling legislation where you did not want me to recreate the National Institute of Health, did not want me to recreate the DOE or DOE labs, you did not want me to recreate the National Science Foundation. But you did give me a preeminent position to go ahead and leverage those tens of billions of dollars of research where those other agencies and departments of government must share with me the results of that critical research so that I can take my precious investment and focus those results on Homeland Security requirements and needs.

That government-wide strategic plan was in preparation apparently for about two years. Because the approach it took, and I have reviewed it myself in draft form, was more perceived by the other departments and agencies as mandated what they would do for Homeland Security, as to how they, through their efforts could contribute to Homeland Security, I think it had a very difficult time coming to fruition. I commit by the end of this fiscal year I will

have to the Administration that strategic plan that is a partnership across government for them then to provide to the Congress.

Chairman WU. Mr. Under Secretary, what I heard you to say is that the first strategic plan that you are going to be working out is going to be informed by shall we say less formal risk analysis. Do you have some plan at this point or some point in the future to do a more systematic formal risk analysis to inform the research priorities of DHS?

Mr. COHEN. Yes, sir. And, in fact, that is in place right now. The reorganization that I put in place where the majority of my budget goes in an integrated product team, to the customer, whether that is border patrol, Coast Guard, cyber security, or infrastructure protection with the National Infrastructure Plan, each of those customers does a risk-based analysis to determine what capabilities they need to fulfill their homeland security mission. Now, you wisely gave us the Homeland Security Institute. In the short time I have been on board I have reoriented them to bring operations research, operations analysis, and make the Homeland Security Institute the risk-based analysis determiner for all of my 22 customers. So when I sit down and integrate a project team and my division director, along with the customer and the acquisition provider, we have 11 capstone IPTs. You see the capabilities they are trying to provide. The customer working with us then prioritizes what they need to do their job based on the risks as they see it. We then commit through technology agreement in writing where they hold me to cost, schedule, and capability metrics to provide the enablers for their people, process, and product. Because that is how they do their job.

Chairman WU. Mr. Under Secretary.

Mr. COHEN. On a bigger scale——

Chairman WU. Mr. Under Secretary, because my time is expiring——

Mr. COHEN. On a bigger scale, I will answer your question directly. I have sat down with the National Academies of Science because, and the other Members may feel differently here, the science of risk is not well known, and I have asked the National Academies to work with me so I can fund how we can better determine risks for the issues that have been raised here.

Chairman WU. Thank you very much for focusing on that part of the question. With the forbearance of the Ranking Member, a few seconds after my time has expired, since you have brought up this chart, I wanted to ask you about the IPT. You know, I think it is terrific that the different federal agencies have been pulled together in this. I have to say that there have been concerns expressed, perhaps some complaints, that some of the end users, and you refer to them in your testimony, and the first responders, that some of their needs in terms of usability, in terms of maintenance, you know, the ability to withstand challenges in the field and prioritization of devices and threats, that that has not been paid sufficiently close attention to, shall we say. And that a specific example would be the, what many of us would consider, you know, shoulder-fired anti-air missiles in this town, MANPADS, man portable air defense systems, that the system that was developed is roughly a million dollars a copy. The folks who would be respon-

sible for purchasing them and maintaining them are reluctant to make that investment. Do we have a problem here with a lack of linkage with the ultimate user?

Mr. COHEN. I will give a concise answer. Yes. This is an area that I am very much focused on. The enabling legislation not only made the head of the S&T Directorate, but you made me the test and evaluation executive for the entire Department, and you put standards, not just inter-operability, but all standards under me for the entire Department. In the IPT process you can see the bottom of each diamond has the customer, the guardsmen, fill in the blank.

Chairman WU. Above the line, those are solid lines, that is a dotted line down below, and I don't know who to interpret that.

Mr. COHEN. Yes, sir. Because S&T is like the BASF commercial you see every Sunday morning. I don't make the widget. I make the widget better. My other panel members already noted, S&T for S&T's sake does not satisfy the customer nor does it reduce the risk to this country. And so what I have done in some cases because they are internal to DHS, I have mandated, because it is my process, the customer, the customer be there. But I am not going to tell the Commandant of the Coast Guard, and I am not going to tell the cyber czar, et cetera. I have provided for the customer to customer to be at the table.

We have also established, and it is operating and running, tech solutions, a website, something I did in Navy, where first responders themselves can come to my website with recommendations or gaps that they believe exist, because they live it every day, and they are smart people. In Navy I had a sailor who came in to from the Persian Gulf on a carrier who asked for a degreasing Zamboni for four and a half acres. It wasn't quite S&T but we provided it, using our laboratories, and that sailor I don't think ever bought another beer in his life. We are going to do the same, and I am committed to our first responders. But this is a work in progress, and I look forward to improving it as we go forward. But you are right, and we have got to do a better job, and I believe we are organized to do that now, sir.

Chairman WU. Thank you very much, Mr. Under Secretary. Dr. Gingrey.

Mr. GINGREY. Thank you, Mr. Chairman. Mr. Under Secretary, Admiral Cohen, I had mentioned in my opening statement a very difficult task to assess and characterize the various threats that our nation faces. In that vein I am interested in hearing more about this BioWatch Program, I guess it is called. BioWatch. Can you give us the history of the program, its various successes, and some of the struggles and what you see as the future of BioWatch? It is my understanding it is a program that can play an effective and efficient role in securing our country, but there has been some problems. So if you would talk to us about BioWatch.

Mr. COHEN. Yes, sir, Congressman. I am a big fan of BioWatch. In fact, Rita Colwell, Dr. Colwell, when she was Director of the National Science Foundation, in the summer of 2001, came to me as Chief of the Naval Research and proposed a cooperative program—Army DOD with her for something very similar to this, so that in our main cities we would put in place sensors that would monitor

for various pathogens. Because we didn't have a database how that varied diurnally with season, what the false alarms were, weather conditions, et cetera. It didn't gain traction, and then we had 911, and then the standup of the Department of Homeland Security.

On the broader issue in terms of the priorities and risks, what I basically inherited was Mr. Oxford has about one-third of the S&T budget for nuclear and radiological. Chem bio has about one-third of the budget. Those are the two obvious, clearly defined, major threats, and all the other threats share about one-third of the budget. Is that right or wrong? I don't know. That is follow the money.

The BioWatch Program was established about four years ago. It was intended to do what Rita proposed. I don't know that they knew she proposed it, but it was to go in about 30 of our major cities, using current technologies with fixed stations to monitor pathogens that we have the technology to do. And it is analog in nature. You know from your background we draw the air through pads, then we collect it weekly. We then go to the lab and do a detailed analysis.

It has been highly successful. It works. We have taken over three million samples of which we have gotten 15 positive results, all of them verified but all due to natural, not terrorist causes. In fact, two months ago when the stink bomb engulfed Manhattan, and we didn't know what it was, smelled like hydrogen sulfide, Mayor Bloomberg, I understand was able in the first hour to go before the good people of New York City and say they didn't know what caused it, but it was not a threat. That statement was in part enabled by the BioWatch sensors in New York.

We have now in the Department of Homeland Security, working in conjunction with the Congress through the last year, established the Office of Health Affairs. That is headed by our Chief Medical Officer, Dr. Runge. Dr. Runge filled in for me over the last six months before I came on board at S&T, and we work very closely together. This is an area where S&T didn't have a customer in DHS. Now I have a customer, and so my budget this year reflects a one-time transfer of approximately $80 million to Dr. Runge and the Office of Health Affairs, because that is what it costs to operate BioWatch II, which is in operation.

Now, we will continue to do S&T to improve that system, but with Dr. Vitko and the rest of my chem bio division, we are leaping ahead. We are leaping ahead to BioWatch III. This brings the current digital technologies, the microchips that will allow us, we believe, when fielded, and we hope to have it fielded within the next three to four years, the ability to have real time monitoring coupled with wireless and hopefully because it is one quarter the cost to operate, four times the sensors in many more cities——

Mr. GINGREY. Yeah.

Mr. COHEN.—so that——

Mr. GINGREY. I know my time is running out, Admiral.

Mr. COHEN. Sure.

Mr. GINGREY. But in the remaining few seconds, tell us some of the particular things that you would be monitoring for that the general public would be aware of, things like sarin gas as an example, or anthrax or something that we read about. Fortunately, on

not a common occasion, but it scares the bejesus out of everybody. Tell us some of the things that you are watching for in these 30 cities.

Mr. COHEN. Yes, sir. I will leave it very limited in this form because you are aware that we did put out earlier or late last year a major threat determination on 30 different pathogens, using a very detailed risk determination, probability of occurrence times consequence of occurrence. But it is safe to say that anthrax, botulism, some of the more common diseases that could be pandemic are monitored for.

Mr. GINGREY. They are part of that watch?

Mr. COHEN. Yes, sir.

Mr. GINGREY. Thank you, Mr. Under Secretary, and thank you, Mr. Chairman, and I look forward to the second round.

Chairman WU. Thank you, Dr. Gingrey. Mr. Mitchell.

Mr. MITCHELL. Thank you, Chairman Wu. Mr. Under Secretary, much of the Secure Borders Initiatives Systems development has been completed by S&T. How have you insured that the Secure Borders Initiative has responded to the needs of customs and border patrol agents along the Southwest border?

Mr. COHEN. Well, Congressman, the borders are clearly very important to us, and it has been a major S&T initiative. Secretary Chertoff has testified numerous times that the current contract for the SBI went with proven technology so that it could be fielded in a timely manner. I know you are well aware of this because of the towers and the other aspects that are being deployed in Arizona and other Southwest borders. In our integrated product team which you see border security, both the customs and border protection and ICE are my chairmen, and it is Chief Aguilar himself who sits at that table with my border and maritime Merv Leavitt, Director. And it is Chief Aguilar and ICE who tell us what they need to make the borders better. We slave it to that.

Now, these, Congressmen, are incremental improvements. These are spiral development. Maybe we can move the towers from five-mile spacing to seven and a half mile spacing but with the same fidelity to insure the safety of the border. And we are doing that. I am investing into that, but in my high-risk portfolio where Dr. Epstein talked about the need to take risks and fail, we have several programs. Tunnel vision, tunnel detection. No one has been able to do this in a timely manner. We are going to risk, we may fail, but in fact, and I think you know him from Tucson, Tony Mulligan, in Advanced Ceramics, is proposing using Silver Fox, a small 24-pound unmanned aerial vehicle, and using, I am not going to give the technology, but fly that along the border to see if we can detect tunnels down to several hundred feet. Will it work? I don't know. Stay tuned. But I get to do that. We are also using persistent surveillance. These are 24-hour, high-end UAVs, unmanned aerial vehicles. We are using them for several reasons. One, as counter MANPADS. As the Chairman said, the airlines are not high on the cost or the maintenance of the impact of counter MANPADS on their aircraft. So we are looking to use a 65,000 foot decoy to take the MANPADS away from the aircraft. But this same decoy can be used with state-of-the-art day, night video to give us persistent surveillance as we have overseas in war on our borders

for our border patrol. And it can also be used as a bounce link to have secure communications, reliable communications in that last mile for a distant franchise, first responders. I know your time is short. What I am telling you is we are taking the low risk and the high risk at the same time to make the borders more secure.

Mr. MITCHELL. Thank you. Just one follow up. Has the border patrol expressed the need for any research and development that has not been completed yet?

Mr. COHEN. Absolutely. In fact, one of the things that I liked, please put that up, about this Integrated Product Team Process, and I learned this in Navy, this is not new, is when you have the customer at the table, they always have, I know this is hard for Congress to believe, always have more requirements than we have money or technology to fill. And so we ask the customer to prioritize. Now, here you are seeing my human factors. My people screening. In the upper left that is what I am funding. These are all prioritized. In the lower right I am funding for those in the out years. It goes to the issue that was raised by Ms. Ward. I am doing six-year funding, and I am showing OMB, and I am showing the Hill how we are sequentially going to invest. And as more money becomes available, those items below the cut line put there by Chief Aguilar, get raised, because I can do them. But the ones that we are doing in zero to three years, when they are delivered, I reinvest that money in the items below the line, and they naturally move up over the six-year budget period.

Mr. MITCHELL. One last quick follow up. How has, there is a proposed cut in the border and maritime division of about seven and a half percent. How will this cut affect the research that is being done there?

Mr. COHEN. Congressman, in going to the new organizational construct, I have basic research, which I am growing. It was at five percent. My goal in my tenure is to get it to 20 percent for the reasons you heard Dr. Epstein address. Fifty percent of my budget goes to the Integrated Product Team, the immediate improvement for my 22 customers, but 10 percent goes to innovation. It is the high-risk portfolio. So what I have done with Merv Levitt and with the Commandant, is we have taken some of the monies that were in what we call on and on research, no defined customer, and we now have Merv Levitt in borders and maritime with a defined customer requirement and the high risk. And so what I have done is it has been an internal transfer of money from that division to my innovation portfolio. But the monies are fundamentally the same, sir. Just differences in risks and time of delivery.

Mr. MITCHELL. Thank you. I yield my time.

Chairman WU. Thank you, Mr. Mitchell. Now my good friend from Texas, Mr. Hall, the Ranking Member of the Full Committee.

Mr. HALL. Thank you, Mr. Chairman, and I think that I probably want to start off, Admiral, by thanking you and thanking you for all the wonderful work you have done, not just for this committee and for this thrust but for this country. I know your background. You are a graduate of the Naval Academy. I never could have got in there, much less getting out. You were MIT, you were Navy Congressional liaison. You have done it all, and I don't know of anybody more qualified for what you are doing and doing it right than

anybody under the Capitol Dome, and I want to thank you for that. We are lucky to have you.

I have a question for you and for Mr. Oxford, and I guess maybe it is general, but just what tools and what procedures are available through your offices to help State and local governments, the people at the bottom, to help them assess and address their own vulnerabilities to natural and to manmade disasters? And how can interested communities interface with expertise as housed in DHS, and how do you get it from your mind down to their mind and to help us defend that that they are obligated to defend just like you are at the top? Would you give me something like that in the last three minutes I have?

Mr. COHEN. Yes, sir. First of all, I want to thank you for your very kind words, but I also want to thank you for your long and dedicated service and especially your focus on science and education. I would like to remind you that our greatest Admiral, Admiral Nimitz, was a Texan from Fredericksburg, and my only regret in life is that I am not a long horn.

Mr. HALL. I was a JG when I served under him. I didn't get any closer than 100 yards of him, but I sure did admire him.

Mr. COHEN. Yes, sir. I am going to give you a fairly succinct answer. The first responders and the communities are not at the bottom in my book. They are at the top, and I exist to fulfill and serve their requirements. We have many, many ways to do that. I briefed the Tech Solutions website, which I put online, where they can come in directly. I have established in my organization, very lean agency, because my responsibilities run throughout all Federal Government and also international. I was going to have an association, because I have to deal with the sheriff in Mayberry, and I have to deal with the New York City Police Department. And I have to deal with the Tribal firemen, and I have to deal with the Chicago Fire Department. That scale is very difficult for me, but as Ms. Ward has indicated, this is the role of the associations. We in Homeland Security have, in the Department, not in my directorate, and I think that is appropriate, groups that reach out to private industry, groups that reach out to associations, sit down with them. They then pass those needs to me. But as I said in my confirmation, my door is always open. At the end of the day the 22 components and agencies, border patrol, Coast Guard, who deal, who live in those communities, they bring to me their requirements tailored for those communities. This is a very difficult issue. We have got 35,000 fire departments of which 80 percent are volunteer. This is how America works. This is the beauty but also the challenge of America. It is a new department. It is a work in progress. I do think we are getting wind under our wings, though, sir.

Mr. HALL. Are you actually in touch with these folks? Do they know a number that they can call? Do they know how to call for help if they see something that concerns them?

Mr. COHEN. I would say that some do. I would say the majority don't. I would tell you that I am not proud of the Homeland Security Department website.

Mr. HALL. But if I know you, you are working on it.

Mr. COHEN. I am. You bet. Yes, sir.

Mr. HALL. And thank you for that. I thank every one of you for not just being here today but for how you got here today, and I have made this statement before. I would have known all of you and would have admired you, but I wouldn't have liked any of you because you are the very people that run the curves for guys like me in college. But I thank you for your participation, and I thank you for what you are doing for this country. All of you. I yield back, Chairman Wu.

Chairman WU. Thank you very much, Mr. Hall. And the Chair now recognizes the gentleman from Kentucky.

Mr. CHANDLER. Thank you, Mr. Chairman. Admiral, I also appreciate your service. Unlike our, my friend, the Ranking Member from Texas who has obviously Texas has somewhat of a tradition with the Navy, with Admiral Nimitz, I am afraid Kentucky's historic association with the Navy is not that great, despite our enormous coastline.

Mr. COHEN. With Ohio.

Mr. CHANDLER. Yes, sir. That is right. The Ohio Ocean. Mr. Under Secretary, I am interested in a cut, a proposed cut in the budget request having to do with University Centers of Excellence. I noticed that the number, the FY 2006, number was $62 million; in FY 2007, enacted $48 million. Now, the suggestion is down to 38 million, and in addition to what is a fairly substantial cut, there, as I understand it there is also a proposal to spread that money over more universities. Could you give me some indication as to the thinking there, and will the money when it is watered down in that way or, you know, less to each place, will that yield as strong a result as you have been getting from those programs?

Mr. COHEN. Yes, sir. And you will never heard me say less is more. This is something I testified to two weeks ago with the Homeland Security Committee. You may remember when I came on board last August there was some less than complimentary language in the pending Congressional legislation about my directorate and more specifically about the Centers of Excellence. Working with both sides of the aisle and both Houses, authorizers and appropriators, we were able to find a solution. But for the Centers of Excellence, draconian measures were about to be taken because of the perceived under-performance as they were organized prior to my arrival. The legislation that came out I am very thankful for. It required me to come back to the appropriators, both House and Senate, within 60 days of enactment, which I did on the 58th day. Chairman, I can meet some schedules. And explain how we were going forward. With my new organizational construct it has six division and three investment areas of basic research, product transition, and high-risk innovation. Everything is aligned to explosives, chem bio, command, control, inter-operability, to borders maritime, to human factors, and infrastructure and geophysical sciences. That is how I do business overlaid by matrix portfolio directors so we don't have stovepipes. In September of last year I sat down with all the directors of the existing seven COEs and asked them to align with one or more division so I could justify their existence in the basic research. They immediately did that, and I am very proud of that. But at that same time the Congress advised me, and I looked at my own six divisions, have we got the vertical? Yeah.

Would you turn that for the Congressman, please, just so we can see it better? I had two divisions that were lacking any Centers of Excellence, and they were critically important. Explosives. And so today I have four broad agency announcements, competitive in nature, to fill those areas that I knew the Congress wanted me to do. And we have consolidated.

On the Administration side, the Administration and the Department and OMB, looking at that pending legislation, which would have decimated the COEs, went ahead and removed as part of the budget development a majority of that funding. That was unacceptable to me, and so I was working, as I said in testimony, a two-front battle. On one hand I had the Congress telling the Administration they are going to do away with it, and on the other hand I had the Administration saying, not even the Congress values them. I was able to buy back, as you can see, 80 percent of what I had the previous year. With this new alignment I guarantee you, and I use that word rarely, that with the product you will see coming out of basic research, the universities and the associated laboratories including Silicone Hollow, which we are very pleased to be involved with, I believe you will see, the administration will understand the value of this, its dual use, and we will grow that budget.

Mr. CHANDLER. Thank you, Admiral. It sounds like you have put a lot of thought into this, and so you got, what you are saying is you got what you could get by what appears to be a lot of hard work.

Mr. COHEN. Yes, sir.

Mr. CHANDLER. I have got one other question, if I may, Mr. Chairman. And this is I think better answered by Dr. Epstein possibly. The S&T Directorate seems to have a strong focus on biological threats that are human caused, things like anthrax, smallpox, that sort of thing. Do you think that this, and I understand how important those are, is this in your view the main priority, or should the priority, or should we be, are we doing enough, let me ask it that way, are we doing enough to prepare for natural threats, naturally occurring threats? For instance, the avian flu.

Dr. EPSTEIN. I think I will echo Under Secretary Cohen's reply that we are never doing enough. There is a lot of threats out there. One challenge with this particular question is that natural threats, well, let me back up. There is two different Cabinet departments involved, and so part of the challenge is not just determining how much money needs to go to it, but what is the relative role of the two departments. And the point I make here is that there is no correct way to make that boundary. These are both, at least on the bio-terrorism side, a bio-terrorist attack is an intentional attack, and it is a disease. You have got one Cabinet department to worry about disease. You have got another one that worries about intentional attacks, and they will both have to be involved. I think it is appropriate that the bio-terror focus that the Department of Homeland Security has is there. I think it is appropriate that is their largest program. When one looks out into the future and says, all the ways that technology can be abused by folks who have ill-intent, what are the capabilities that might put the most power in the hands of the smallest groups in the most places. Biological

weapons are certainly one that is a serious problem. No matter how serious one thinks it is today, it is not getting any better in the future.

The pandemic natural disease problem, again, it is something that we have to expect we will see. Parts of the government are mobilized to do it, and I, it is hard to give a short answer as to whether we have the right balance. I mean, I think they are both important, and I think they both are getting attention, and we just need to keep our eyes open to them.

Chairman WU. Thank you very much. The gentleman from Texas.

Mr. HALL. Mr. Chairman, thank you. When I asked the Admiral a question that I asked a few moments ago, I noticed Ms. Ward gave me an eyebrow there, and I want to follow up with her and leave little enough time for Mr. Oxford maybe to tag onto it, too, because I asked those two the question, but I think you probably have more real experience at the level that I am talking about, because I note in your background that you have been in the trenches at the local level, and you were in the city management business for the city of Orlando. Probably, I was stationed there in 1943, at Daytona Beach, and drive over to Orlando. The magnificent growth at that time, you were part of that. And city managers are kind of like tail gunners. They are usually removed after each mission, and if you survived that, you had a lot of good experience there.

I want to ask you——

Ms. WARD. It has changed a lot.

Mr. HALL.—to help us with that. I note that you were a task force leader. You were a coordinator of a regional area, and you have been early days in public safety. Now, for a little community like Blackland or Munson in my home, I live in the smallest county in Texas of 254 counties, and we would be a great one to test to see how far really what the Admiral's working 23 hours a day on, reaches us. Give me some ideas as to how we can, I can tell folks there that I see day in and day out, that I go to church with and see on the streets, how they could benefit from what all five of you are doing?

Ms. WARD. I was very happy to hear the Admiral acknowledge the fact that some of the local people probably don't know what is going on, because that is a very true statement. That is one of the benefits of the group that I belong to, and I had not seen the tech solutions website and will be happy to provide outreach to the membership and their members so that they will know that that is available. That is one of the hardest things that we deal with is getting back down to the trenches.

Mr. HALL. It is the figures, the numbers alone just are stultifying.

Ms. WARD. That is correct. And that is actually the value of our group, the NPSTC group.

Mr. HALL. Yes.

Ms. WARD. Our associations represent all of these people, so what we end up working with SAFECOM on, goes back into our associations, and then is funneled down to the lowest level, including the volunteer fire departments that were referenced earlier. That is why we are hoping that this esteemed group will see the

value of what we do with the SAFECOM group, take into consideration the 9/11 Commission's recommendation, Secretary Chertoff has also said that inter-operability is going to be one of the major issues to get resolved and kind of not dilute the message that we, and our mission by changing the personality of SAFECOM. Because those people that work in your community, the public safety people, the only way they are going to be able to get reached is through some mechanism where the State and local people have input into what is going on here in Washington. And I will tell you, you know, I come from local government. I would never have any funding to be sitting in this chair from Orange County where I worked or the City of Orlando if it was not for the associations that were supporting me to be here. So that is a major issue that this committee and Congress in general I hope will take into consideration that you have to find a means to be able to get local and State participation, and the means is through the associations and through supporting groups like ours that bring associations together.

Mr. HALL. And the means are green, aren't they?

Ms. WARD. Yes, sir.

Mr. HALL. And that is what, where we are supposed to come in.

Ms. WARD. Yes, sir.

Mr. HALL. Mr. Oxford, if I have a minute or so left, do you want to add to that?

Mr. OXFORD. Yes, sir. First of all, I want to point out that when we stood up in my office, we acknowledged the need to have an aggressive dialogue at the State and local level. I have an office director for State and local affairs that reports directly to me. Since that first day we have had an aggressive outreach through a series of workshops at the State and local level. Just a month ago we had a series of telephone conferences that engaged 34 separate states, about 150 people, starting with homeland security advisors on down, to talk to them about the threat, about their problem, the things they could bring to this table. In concert with that we have done specific commercial off-the-shelf testing for State and local people that are interested in acquiring radiation detection equipment. We then post those results on the first responder knowledge base, so they all have access to the test results so they can make these acquisitions in an informed way.

As they acquire this equipment we also have established a training program where we write the curricula for how to use these devices. Using grants and training funding then, we are allowing delivery at the State and local level to the people using the equipment so they know how to do that. In a like manner we have set up a series of pilot programs in the Southeast, and in the Northeast we have established regional technical support laboratories so if they have an alarm, they have someone they can call to get the alarm resolved. They can also call my joint analysis center directly to understand what to do with the alarm information that they have.

So we have had an aggressive program. I have a director for operations who is a senior FBI agent. He is working now with all the JTTFs as well as all the fusion centers that are evolving across the country to bring out relevance to each of those states. So we can

talk a lot more in detail later, but we have had an aggressive State and local outreach.

Mr. HALL. Well, I thank you for that information. It is a wonderful thing, and I have noticed so many times at the local level that, for example, a lot of times you don't even fix a bad bridge until a teenager gets killed there, and then that brings it to your attention and why haven't you done it before, and when did you know the bridge was bad? We are going through that with the hospital out here about 100 miles from here, right today, at the federal level. Information is really great, and you all have a major job of making that information, sifting it down to the local levels where they can use it and have it available if it is there, and I thank you for it. I yield back, sir.

Chairman WU. Thank you very much, Mr. Hall. Pardon me. I want to apologize first to the three other witnesses. I intend to bring you in right now, well, in a moment, to address the risk assessment issues, which the Under Secretary talked about during my first round of questions. But before I do that, Mr. Oxford, I heard the Under Secretary refer to you as Dr. Oxford. And if we, if this subcommittee has deprived you of a Ph.D., I deeply apologize, and let me just refer to you as Director Oxford.

And the question I have for you is that in your testimony you have referred to a research agenda that is at least in part driven by end user requirements. However, specifically with respect to the Securing the Cities Initiative, there have been publicized reports, *The New York Times,* among others, that DNDO is not addressing the cost and maintenance and other requirements of local governments who ultimately will be responsible for paying for the equipment, its operations, and maintenance. Is there a formal structure for the ultimate end users to have their say in the technologies that you are not only developing but apparently deploying in the Securing the Cities Initiative?

Mr. OXFORD. Well, thank you for both those questions, and with the absence of the Ranking Member I will say that I am Mr. or Director, and I work for a living so I never went on to the other academic pursuits. But I take those as accolades.

We have a very aggressive program with the New York City officials. This is a developer, user combination. My counterpart in New York is the deputy commissioner for counter terrorism as designated by the actual police commissioner in New York. Mayor Bloomberg has delegated the radiation detection issue to Ray Kelly, the police commissioner. He, in turn, has delegated this to his counter terrorism deputy commissioner. He has formulated a structure within the New York region of bringing together all the major entities that exist within New York City as well as New York State, New Jersey, and Connecticut at this point in time. They have veto authority on any potential deployments that we have to that region. This is an active dialogue where we are building a deployment architecture that will be predicated on system capability as well as their ability to actually operationally respond to any alarms. We can't just have detectors in place that have alarms that they do not have the operational capacity to respond to.

So it is a strong, mutual dialogue. Them having veto authority over any potential deployments that we might make, as well as

they will observe any testing that we do on the systems to make sure they work in the capacity of how they want them to work within the city before we deploy.

Chairman WU. Well, Director Oxford, the veto authority is great, but one hopes develop the technology that everyone can use rather than having a veto so that it is not deployed.

As we turn to the other three witnesses, you know, I am going to cite a few numbers here, and we did this quickly, and this is, I only gave the staff a few hours to pull this together, and this is down and dirty. As the speaker said in the meeting last night, in her time on the Intel Committee, the plural of anecdote is not data, but this is slightly better than anecdote and not as thorough as a real risk assessment.

According to the numbers that we pulled together, computer consulting firms estimated that total economic loss of all forms from cyber attack in 2003, was $226 billion. That, I will skip a number of these other related statistics. That the insurance industry estimates that financial losses due to a tsunami could be up to $100 billion, that weather-related losses between 1980, and 2005, in the United States alone according to NOAA, is over $500 billion, and I will skip the numbers pertaining to deaths from explosives as opposed to other causes in human-caused incidents.

But I am deeply concerned about the proper integration of formal risk analysis and we understand that there are some challenges there with good solid risk analysis. But I would like our, if you will, outside witnesses to talk with me a little bit about this and how we could better integrate the risks that we face with the research that we are doing so that we properly face the threats of the future.

Dr. EPSTEIN. Any of us just jump in?

Chairman WU. Why don't we start with you, Dr. Epstein.

Dr. EPSTEIN. You have got your finger on a terribly important problem, and it is a terribly hard one. Let me back up a little bit. Much of the methodology we have to make this kind of calculation today comes from looking at engineered systems. We have a whole science of nuclear reactor accidents, probability of risk assessment. What is the probability this valve will fail, this pipe will burst? Another branch that we are drawing from is sort of looking at infectious disease, natural-occurring incidents, weather, things were we have a database, things where we have statistics, things where nature isn't going to change what it does because we do something.

We have got a very different problem here looking at the intentional threat. We have got adversaries that are looking not only at what we are doing in and where we are weak. They may look at the output of our risk assessment, which says we think risk A is high, we think risk B is low, and they may hit us on risk B. So in principle this is a much more difficult job than anything that has looked like risk assessment or probabilistic analysis before. And my comments on the field are not so much that I think there is a lot of things we need to do to figure out how to handle the problem. It may be cautionary that it is a terribly important question, and there may be fundamental limits on what analysis will tell us.

So the type of approach I like to see is structures that help guide our thinking. We will never know what the right number is for the probability of a terrorist attack, let us say, but we have to have a system where if I think it is high, I jack it up. If I think it is low, I jack it down, and I get to see what happens on other parts of my portfolio. I do think we have the right institutions involved. If the National Academy of Sciences is gearing up to look at what is the state of science in this field, they have the ability to tap those people in the academic community. The Homeland Security Institute that Under Secretary Cohen mentioned was created by, suggested by act of Congress, created by DHS, with these specific types of questions in mind. If that power can be devoted to looking at these questions, then we have got the right analytic skills and the ability to draw on the people, who, if there is an answer there, one would hope they are able to come to it.

But my basic point is this is a very different question than what we have been trying to do in the past when we have been doing things that sound similar.

Chairman WU. Thank you, Dr. Epstein. For the next two witnesses, my apologizes to the panel in general. Those bells and whistles that you all have been hearing, I mean, it could be worse. The ship could be sinking, but we have just been called to a vote. That was a few minutes ago. We have about five minutes left for the vote. So if you all could try to make your comments in about a minute or so that would be deeply appreciated. Mr. Czerwinski.

Mr. CZERWINSKI. I will be brief. Let me just try and reframe the issue in this way. Risk is different in homeland security than it is in anywhere else. The reason for that is that what is at risk is just about everything. If you think about what the DOD has or what the Defense Department has to worry about in terms of pursuing its objectives, it worries about its own combatants, it worries about non-combatants, and it worries about the enemy. Well, in homeland security we are worried about everything else. The global economy is a part of the equation, so we have to look at this in such a way where we can't just say, well, the risk is this. We have got vulnerabilities, and we have got threats against those, so now we have risks. Instead, we have to take a look at much, much broader picture, at the impact of the certain A, B, or C level types of vulnerabilities that Dr. Epstein was talking about and say what would the consequences on these. That is really where risk comes out.

The impact of certain attacks is one thing but also the impact of the measures we use against those attacks. An overreaction in homeland security by the U.S. Government could be even worse than the actual attack itself, and we have seen this in the past.

What IBM has been doing now for a few years is actually modeling and simulation exercises that show what these sort of impacts might be, actions and the impact of those as well in certain cases of pandemics, but now we are looking at one in terms of global trade and travel flows as well.

So we can go into this at another time, but I would just suggest broadening the picture in that way. Thank you.

Chairman WU. Thank you.

Ms. WARD. This is an interesting question for someone who represents first responders. We respond as things happen, immediately. Risk assessment comes through different groups like in Florida. I was on the Regional Domestic Security Task Force, where we brought in different entities and different agencies to talk with us about how our ports, I found this discussion today quite interesting because those are some of the same things that we were dealing with on the local level.

Our first responders are reactionary. We have to wait until the phone rings basically telling us to go to a 911 call. We have to look at our crime stats or our fire stats to do fire prevention. So we are not in the same role as some of my co-panelists. But I will tell you that in our work with these other entities, one of the number one priorities for us is that we can talk to them.

So I will come back to the inter-operability discussion and just kind of wind up by hoping that this committee will look at the value of the first responders. They are the first ones on the scene, long before any assistance comes from the State or federal level, and these are the people that we need to take care of. And our interest in inter-operability is taking care of them so that they will be able to talk to each other and ask for help when they need it.

So we would ask that you look at our groups, look at our associations, and look to supporting our programs that allow us to have input into the federal level.

Chairman WU. Thank you very much, Ms. Ward. Thank you for your work. Thank you all for your fine work. We look, this committee looks forward to working together with all of you over time to improve the processes at which we can best identify threats to our nation and to ameliorate them as best as possible. Perhaps there were those, Mr. Czerwinski, you hit on the point that our national defense is focused on one set of issues, whereas homeland defense is focused on so many more. Perhaps there were those who predicted or at least said it was possible for a Japanese military strike at Pearl Harbor in 1941. Maybe yes, maybe no. I haven't looked at the history closely enough to know that. I know that through all the time that I was growing up this nation was preparing for another bolt out of the blue, and we were probably looking the wrong direction, except for perhaps just a few people when the bolt out of the blue finally came. It is our job to try to do our best, do our level best to have the technology and the people in place to prevent that from happening, to do what we need to do.

I want to thank all the witnesses for being here today, and I now need to bring this hearing to a close. I want to thank all the witnesses for testifying. It has been highly educational. I look forward to working with the agencies and working with our outside information sources.

If there is no objection, the record will remain open for additional statements. Hearing none, so ordered. Members, questions will be submitted and answers may be given for the record. Without objection, so ordered. This hearing is now closed.

[Whereupon, at 11:49 a.m., the Subcommittee was adjourned.]

Appendix:

Answers to Post-Hearing Questions

ANSWERS TO POST-HEARING QUESTIONS

Responses by Jay M. Cohen, Under Secretary of Science and Technology, Department of Homeland Security

Questions submitted by Chairman David Wu

Staff

Q1. In your written testimony, you stated that you have hired 66 percent of your full staff.

Q1a. In which divisions or offices do you lack staff? Do you have adequate mid-level employees to support your Directorate's day-to-day activities? What impact does this have on operations and how will things change when you are fully staffed? What percentage of your current staff are detailed from other federal agencies? Of those detailees, how many are in senior level positions?

Q1b. In which divisions or offices do you lack staff?

A1a,b. Program manager and program execution functions across the S&T Directorate are not fully staffed by federal employees; however, they are better staffed now than prior to the ramping up of S&T Directorate hiring efforts at my direction. The bulk of our hiring actions are focused on bringing on program management expertise and building the next generation of senior program managers.

Q1c. Do you have adequate mid-level employees to support your Directorate's day-to-day activities?

A1c. The S&T Directorate supports its day-to-day activities by supplementing its federal staff with contractual support and some detailees from other federal agencies and other entities, e.g., national laboratories and State and local governments. The S&T Directorate's goal is to further solidify this staff by increasing the ratio of federal employees to contractual staff.

Q1d. What impact does this have on operations and how will things change when you are fully staffed?

A1d. As the S&T Directorate builds its federal staff, it will create more permanency and build morale, leading to retention of valuable employees and institutional memory, which helps to maintain consistency and improve efficiency.

Q1e. What percentage of your current staff are detailed from other federal agencies?

A1e. As of pay period three, the S&T Directorate had 262 FTE. The detailed staff equates to six percent (a total of 17 employees).

Q1f. Of those detailees, how many are in senior level positions?

A1f. One detail employee is in a senior position.

MANPADS

Q2. The request for the explosives account is reduced significantly in the FY 2008 budget, due to the end of funding for the counter-MANPADS program. However, there have been a number of news reports about airlines being uninterested in purchasing counter-MANPADS technology because of its purchase price and high maintenance costs.

Why is R&D for counter-MANPADs technology being discontinued before it can be manufactured and maintained for an acceptable cost to end users? What are the lessons learned from this program and has the S&T Directorate changed its technology development programs as a result?

A2. As directed by Congress, the objectives of the program's final phase, Phase III, include establishing a better basis for estimating the sustainability costs for systems derived from military technology. To go further and achieve manufacturing, maintainability, and sustainability costs acceptable to end users would require substantial investment across multiple years, which is beyond the scope of the S&T Directorate program as defined by the Congress.

Congress directed DHS to develop and demonstrate military Counter-MANPADS technology for protecting commercial aircraft, which the program has accomplished. Counter-MANPADS has been a very successful program resulting in two systems that could protect commercial airlines if deployed. This program employed a rigorous systems engineering approach using knowledge-based acquisition principles.

Among the important lessons learned are: a comprehensive test and evaluation program must fully account for the operational environment; that life-cycle costs must be addressed early and completely; that modeling and simulation produce substantial dividends; and engaging all stakeholders early and often is crucial to success. This has proven to be an excellent model for major systems development programs, which the S&T Directorate would follow for similar programs that are meant to be carried all the way to a deployment decision. Many S&T Directorate programs feed into broad pilot programs managed by the Transportation Security Administration (TSA), which would carry the technology to deployment for use by TSA agents and first responders. In such cases, the S&T Directorate would develop the technology to a level appropriate for use in pilot deployment projects.

The developmental phases of the Counter-MANPADS program will end in early 2009, with Phase III in-service operational suitability evaluations in cargo and passenger airline environments.

MSIs

Q3. You mentioned in your testimony that some funding for the University Centers of Excellence and scholarship and fellowship programs will go towards increasing the participation of under-represented minorities and minority-serving institutions (MSIs) in these programs.

Q3a. What is the current level of participation by under-represented students (including women and minorities) and MSIs? What are your specific plans for outreach to and retention of these groups in the S&T Directorate's education programs?

A3a. Currently there are 255 students participating in the Scholarship and Fellowship Program at the undergraduate and graduate levels. Of that number 44 percent or 115 are women and 39 students identified themselves as under-represented minorities. Please note that providing information on race and ethnicity is voluntary, therefore not all minority students may have been identified. Since the inception of the Program in 2003, scholarships and fellowships have been awarded to 17 students from 13 Minority Serving Institutions (MSIs): 11 students from Historically Black Colleges and Universities (HBCUs) and six students from Hispanic Serving Institutions (HSIs).

Q3b. What are your specific plans for outreach to and retention of these groups in the S&T Directorate's education programs?

A3b. In FY 2007, the S&T Directorate established the Minority Serving Institutions (MSI) program to enhance outreach, recruiting and retention. The MSI initiatives are designed to improve the capabilities of MSIs to conduct research in areas critical to homeland security, develop a new generation of scientists capable of advancing homeland security goals and aid in faculty retention in the broad area of homeland security science, technology, engineering and mathematics (HS–STEM). Competitive incentives will be used to integrate the MSIs with the DHS University Centers of Excellence, to develop homeland security research and training capabilities at the MSIs, and to develop career pathways for MSI HS–STEM students at DHS, State and local agencies, national laboratories and Centers of Excellence. Finally, the program will develop internship and career opportunities at a variety of DHS venues.

Program activities include:

- Conducting a Summer Research Team (SRT) Program for MSI that provides a 10–12 week summer research experience for teams, consisting of a faculty member and up to two students, to perform research at a DHS University Center or Excellence (COE) that aligns with the DHS mission. The program began in 2005 and to date there have been 16 teams and 43 faculty and students from 15 MSIs who have participated in the program. Several of these SRT projects have evolved into longer-term and more extensive partnerships between MSIs and existing COEs Team selections for 2007 are in progress.
- Sponsoring a Summer Workshop on Teaching Terrorism for faculty and graduate students at Minority Serving Institutions (MSIs). The workshop will: 1) offer an intensive short-course on the fundamentals of terrorism; 2) introduce academics to new and innovative techniques utilized to teach terrorism; and 3) provide access to high-level officials working in the intelligence and counter-terrorism fields. It will also feature expert specialists from the Centers of Excellence and integrate curriculum content from the DHS Centers of Excellence including material on the social-behavioral causes and con-

sequences of terrorism, terrorism risk analysis, food security, zoonotic disease defense, and catastrophic event preparedness and response.

- Establishing DHS HS–STEM Leadership and Career Development Grants to MSIs to support programs in critical HS–STEM areas. These programs provide MSIs with funds to support early career faculty to establish or expand education, research and training activities in HS–STEM areas. The faculty awards are closely linked to scholarship and fellowship awards to qualified undergraduate and graduate students in related homeland security STEM disciplines who intend to pursue homeland security professional and scientific careers.

The S&T Directorate conducted further outreach efforts in 2007. University Programs hosted three regional MSI workshops, which took place on February 4 in Baltimore targeting Historically Black Colleges and Universities (HBCUs), on February 21 at Broward Community College (Florida) targeting Hispanic Serving Institutions (HSIs), HBCUs and MSI community colleges, and on February 28 at USC (California) targeting HSIs and Tribal Colleges. At these workshops, DHS:

- Introduced the MSIs to four new solicitations for Centers of Excellence (COE), explained the opportunities those represent and encouraged the MSIs to submit proposals as lead institutions and as partners;
- Explained the ideas and expectations for the new MSI program that U/S Cohen initiated, and solicit the MSIs input. Note: UP revamped the MSI Leadership and Career Development Grant program significantly in response to comments received from MSIs at these workshops;
- Described the 2007 Summer Research Team program and opportunities for partnerships with COEs;
- Described DHS Scholarship and Fellowship Programs and the DHS Postdoctoral Research Associateship Program; and
- Invited the MSIs to a ten-day summer workshop on teaching terrorism (SWOTT) specifically developed for MSIs. Note: DHS is supporting the attendance of interested MSI faculty to this workshop until capacity is reached.

Other UP MSI Activities have included:

- Participation in the White House Initiative on Hispanic Serving Institutions (HSIs) conference planning committee in Fall 2006;
- Meeting with Hispanic Association of Colleges and Universities and HBCUs at their annual meetings and, at UP's requests, met on ways to disseminate information, engage HSIs and HBCUs, and present at their major conferences;
- Participation in a workshop for Native Americans on the risk of terrorism for Casinos;
- Meeting with a number of other federal agencies on ways to collaborate and leverage MSI resources;
- Collaboration with the White House Initiatives on HBCUs and TCUs on ways to disseminate information and provide speaking opportunities at their key venues; and
- Reaching out to MSIs to encourage MSI students to apply for DHS Scholarships and Fellowships.

In addition, the Department wants to enhance the role of MSIs within the COEs by increasing both the number and extent of institutional partnerships between MSIs and the COEs; either through new COEs, for which MSIs could be lead institutions, or by expanding the network at existing COEs. The current COEs have a total of 15 MSI partners.

Human-Technology Interface

Q4. The newly created Human Factors division within the S&T Directorate could potentially save DHS millions of dollars by providing "Human-Technology Interface" testing services that could help determine whether technology was easy to use and socially acceptable.

What are your plans for leveraging this capability?

A4. The creation of the Human Factors Division within the S&T Directorate reflects the leadership's recognition that integrating human factors elements early in the Research and Development (R&D) process can increase the effectiveness of tech-

nologies and decrease long-term costs. Utilizing the capital available in the Human Factors Division, the S&T Directorate is working to embed human systems elements into all phases of the R&D process, from the basic and applied research stages to the formulation of acquisition guidance. We are also working to leverage the resources of our partners at the Department of Defense, NASA, the FAA, and the national labs—including the work being done at the Transportation Security Lab—to inform and enhance this work.

The S&T Directorate also includes human-technology interface as a key component in the qualification and certification of security screening and detection technologies. For example, extensive human-technology interface assessment of handheld metal detectors was conducted prior to their qualification and procurement by the Transportation Security Administration (TSA). Further, recognizing that incorporating human factors elements into each system it deploys is critical, the S&T Directorate is formalizing, through the establishment of a Community Acceptance of Technologies Panel, the already routine interface DHS programs have with first responders and the American public.

Transportation Security Lab

Q5. I understand that the Transportation Security Lab (TSL) would like to offer its testing and evaluation services to private entities for a fee.

What is your opinion of this idea? Why should the Federal Government offer these types of testing and evaluation services instead of the private sector?

A5. The S&T Directorate is open to the concept where DHS Laboratories, such as the Transportation Security Lab (TSL), would perform testing and evaluation services for a fee and on a confidential basis. It is important that our unique facilities and testing expertise be made available to commercial industry and others for the impartial testing of technologies being deployed at the Nation's airports to screen baggage. Currently, TSL and other DHS labs bear the entire costs of performing services that benefit baggage inspection equipment manufacturers. By adopting user fees, we are not seeking to compete with private industry in any way. Rather, we are seeking to offer industry the use of the unique DHS facilities and skilled personnel on a not-to-interfere basis.

Questions submitted by Representative Phil Gingrey

Projects

Q1. The S&T Directorate actively pursues high-risk, high-yield research and development activities through the Office of Innovation, with the explicit expectation that many of these projects will fail.

How will the Directorate choose projects to pursue in this office? What processes are in place to ensure that projects that are not coming to fruition are in fact terminated?

A1. The Director of Innovation/HSARPA works closely with the Under Secretary for Science and Technology, the Division Directors, other Portfolio Directors, industry, academia, other government organizations, and other sources to determine topic areas for projects. The Director utilizes many sources for guidance including:

- DHS Goals and Priorities as described by the Secretary of Homeland Security;
- Office of Management and Budget (OMB) and Office of Science and Technology Policy (OSTP) Research and Development Budget Priority Guidance;
- Goals set by the Under Secretary for Science and Technology;
- Congressional Direction; and
- Our Customers, the agencies and agents that are on the front lines of DHS law enforcement and protection services. Through the IPT process they are already providing us with their list of needs. If we believe there is a potential solution that may be high risk but would revolutionize the way the need is met, either by greatly increasing performance and capability or by reducing the procurement and maintenance costs, we may decide to select that project for accelerated prototyping.
- Our Vendors, we have received some very innovative ideas from industry, from DHS labs and national labs in the war on terrorism. If these ideas are

such that they would provide leap ahead capabilities if successful, we consider them for Office of Innovation execution.

All the projects that are executed under the Office of Innovation will have program plans and schedules developed that include milestone events, and exit ramps if the technologies do not appear to be progressing. The S&T Directorate will hold periodic reviews for all programs, including innovation, and the decision to continue a program or terminate will come from the senior staff involved in those reviews.

Coordination Activities

Q2. Your testimony identified ways in which the S&T Directorate coordinates with other agencies and groups throughout the Federal Government. Similarly, Mr. Oxford identified coordination activities undertaken at DNDO in his testimony. However, neither of your statements mentions coordination activities between DNDO and the S&T Directorate.

Do you consult with DNDO for strategic planning and budgeting purposes? What mechanisms exist within the Department of Homeland Security to coordinate and balance the activities of the S&T Directorate and DNDO?

A2. S&T and DNDO continue to have a close relationship within the Department and do coordinate efforts at all levels from the shared use of the radiological and nuclear expertise at the Environmental Measurements Laboratory (EML) to the integration of requirements and system development of technologies for use in Departmental initiatives such as Secure Freight. The overarching missions of the two agencies are clearly delineated and therefore do not require a formal collaboration during strategic planning and budgeting activities there are multiple working level interactions that incorporate requirements and de-conflict overlapping and collocated sensor and architecture development programs. DNDO was also invited to participate in the S&T IPT process to provide them out-year program insight and a sense of Departmental priorities in the R&D arena.

Improving Methodologies

Q3. Dr. Epstein suggests that improving methodologies for determining which threats to address and how much to spend on each should be a high priority for the government.

What activities do you have in your organization to address the need for decision-support and long-term strategic planning? What interagency efforts are underway to plan across disciplines and threats?

A3. The foundation for the S&T Directorate's overall decision-support approach is the Planning, Programming, Budgeting, and Execution (PPBE) process, which initiates and monitors S&T Directorate programs and ensures that these programs result in a focused effort to improve homeland security through science and technology. The S&T Directorate's PPBE process uses risk-informed assessment tools to inform the development of program priorities, and to focus efforts on addressing high-consequence threats. The Homeland Security Institute (HSI) has developed an independent model to assess the potential for S&T Directorate programs to reduce homeland security risk and this model has been used to evaluate programs based on an adjustable set of criteria which can inform the S&T Directorate's PPBE process. This model estimates S&T Directorate program contributions to existing homeland security capability gaps while weighing the homeland security risk reduction value of the programs.

The S&T Directorate is committed to delivering capabilities that DHS components can rely on to meet their operational needs. To accomplish this, the S&T Directorate facilitated Customer-led Integrated Product Teams (IPTs) to identify homeland security capability requirements across the Department. Approximately half of the S&T budget was dedicated to developing products identified by DHS customer-led IPTs that established capability gaps and requirements to drive and inform the research and development (R&D) efforts of the S&T Directorate. These gaps will enable the S&T Directorate to identify key customer-oriented programs. In meeting these customer capability requirements, the S&T Directorate draws on the best technologies and technology researchers and developers from across the homeland security research enterprise ranging from the private sector to other government agencies, to universities, to international allies. The S&T Directorate has already put in place numerous interagency Memoranda of Understanding to ensure efficient coordination between the S&T Directorate and other federal, State and local agencies; and the S&T Directorate has Divisions dedicated to Interagency and International collabora-

tion. In executing its balanced portfolio of investments (from basic research to technology transition), the S&T Directorate is determined to be the model customer-focused, output-oriented, full-service science and technology organization that delivers significant value and supports and enhances DHS mission success.

Questions submitted by Representative Judy Biggert

Protective Measures

Q1a. How is DHS implementing its responsibility to analyze critical national infrastructure vulnerabilities and to implement protective measures?

A1a. The Science and Technology (S&T) Directorate provides analysis of critical infrastructure vulnerabilities and supports the implementation of protective measures through its Critical Infrastructure Protection (CIP) Modeling, Simulation and Analysis (MSA) program. Activities carried out through this program include risk-informed prioritization of strategies and resource allocations in support of the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets. For example, one project within the program, the Critical Infrastructure Decision Support System (CIPDSS), provides risk informed insights for making critical infrastructure protection decisions by considering all 17 critical Infrastructures and their primary interdependencies. Once fully developed, the CIPDSS will assist decision-makers in making informed choices by computing human health and safety, economic, public confidence, national security, and environmental impacts. The CIPDSS will transition to the DHS's National Infrastructure Simulation and Analysis Center (NISAC) for operational use in FY 2008.

Q1b. Why has DHS chosen to fund certain of its infrastructure risk assessment and analysis research at the national laboratories on a year-to-year basis rather than a "line-item" budget basis?

A1b. We have recently realigned the S&T Directorate's budget to match the S&T Directorate organization and to map S&T Directorate programs more directly with the components and missions within DHS. This provides our customers and congress with more transparency to our budget and activities. The incorporation of risk assessments and the analysis of critical infrastructure sectors into S&T Directorate programs require a holistic program approach, which relies on understanding existing, emerging and perceived threats. A line item for risk assessments would not align those activities with the programs they support.

Q1c. What is the division of labor among the various laboratory programs in this effort?

A1c. Argonne National Laboratory (ANL), Los Alamos National Laboratory (LANL), and Sandia National Laboratories (SNL) all participate in CIPDSS's development. Tasks related to program coordination, development of system architecture and tools, and prototyping and deployment will be performed by all of the laboratories. Tasks related to consequence model development will be emphasized at LANL and SNL. Decision model development will be emphasized at ANL.

Q1d. How do you distinguish one lab's function and capabilities from another's?

A1d. The S&T Directorate, through collaborative interactions, works with the national laboratories to identify which laboratories have the functions and capabilities that are most suitable for specific programs/projects carried out by the S&T Directorate.

Q1e. What provisions has DHS made for communications connectivity and shared access to common databases among the laboratories?

A1e. The S&T Directorate arranges communications connectivity and shared access to common databases among the laboratories based on program/project needs. One example is the CIPDSS program, in which participants communicate regularly and share data, models, and results through multiple mechanisms. This includes weekly conference calls that include all three participating national labs and quarterly face-to-face meetings that include most technical members. Tri-lab team members share data through the Knowledge Management (KM) portal hosted at SNL. Papers, technical communications, and working papers are shared through the KM portal. System models are shared through web-based Concurrent Version Systems repositories. Lastly, data resulting from computer simulation runs are automatically shared across the tri-lab team using automatic database synchronization mechanisms.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Vayl S. Oxford, Director, Domestic Nuclear Detection Office, Department of Homeland Security

Questions submitted by Chairman David Wu

Detailees

Q1. You mentioned in your written testimony that you have detailees on staff from other federal agencies, including the Departments of Energy and Defense.

What percentage of your staff is detailed from another agency? How do you ensure that interagency personnel are not improperly involved in making grant money available to their home agencies? For example, what conflict-of-interest rules and guidance are in place at DNDO?

A1. Currently 40 percent of DNDO staff members are detailees. Of this, 29 percent are interagency detailees from the Departments of Energy (DOE), Defense (DOD) and Justice (DOJ/FBI), as well as the Nuclear Regulatory Commission (NRC). Detailees from the Department of Defense include officers and civilians from the Army, Air Force, Navy, Defense Threat Reduction Agency, and the Under Secretary of Defense for Acquisition, Technology and Logistics. In addition, DNDO has detailees from other DHS Components such as the U.S. Coast Guard, Customs and Border Protection, and the Transportation Security Administration, which make up the remaining 11 percent of the detailee staff.

Interagency personnel are subject to Department of Homeland Security Management Directive 0480.1, Ethics/Standards of Conduct; Executive Order 12674, Principles of Ethical Conduct for Government Officers and Employees; and 5 C.F.R. Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch. The DHS Ethics Office provides mandatory initial ethics orientation to all new employees, including detailees, as well as mandatory ethics training on an annual basis. In addition, detailees are not allowed to make funding decisions that affect their sending organizations. DNDO's budget and contracting offices are independent from the program offices in which detailees reside. Furthermore, grants would not be provided to other federal agencies (the source of DNDO detailees).

Student Interest

Q2. You pointed out in your testimony the serious problem with decreasing student interest in the field of nuclear science, and I am pleased to see that you are working with the National Science Foundation to provide funding for students interested in this field.

How do you plan to make sure students who take advantage of this funding opportunity choose to go into go into homeland security-related positions, especially at DNDO? Also, what is the actual job market for people with these degrees? What studies or analyses indicate strong demand for nuclear scientists? How many graduates in nuclear science do we need each year, and at what level (Bachelor's, Master's, or Ph.D.)?

A2. As stated in the testimony, the nuclear science community is forecasting a need for approximately 100 additional new Ph.D.s per year in order to fill the overall demand, which includes homeland security. Historically eight to ten percent of nuclear scientists go into homeland security-related positions and we expect this percentage to remain the same or increase. Research and development for homeland security is performed at national laboratories, companies, and universities by nuclear scientists who have broad interests, not just security. Through its Transformational R&D Directorate, DNDO is reaching out to this research community with a combination of Broad Agency Announcements, Calls for Proposals, and National Science Foundation (NSF) solicitations. We do not require nuclear scientists who receive awards under the Academic Research Initiative (ARI) to join DNDO, but we do expect them to join the nuclear science community, whose work contributes to DNDO's programs and activities.

The job market in nuclear science is improving with opportunities in homeland security, medical applications, basic research, defense, etc. An increasing number of nuclear scientists are being sought by DOE, Nuclear Regulatory Commission (NRC), Environmental Protection Agency (EPA), Food and Drug Administration (FDA), DHS, Defense Threat Reduction Agency (DTRA), and the intelligence agencies. In addition, many universities' nuclear engineering departments are seeking new fac-

ulty members and department heads. The American Nuclear Society's Special Committee on Federal Investment in Nuclear Education found "nearly uniform anecdotal evidence that the current production rate for NSE (nuclear science and engineering) graduates is not sufficient to meet demand."

In November 2004, the DOE/NSF Nuclear Science Advisory Committee recommended that the number of new Ph.D.s in nuclear science be increased by 20 percent over the next five to 10 years. The need for additional graduates with Bachelor's and Master's Degrees is assumed to be in a similar, 20 percent range.

The shortage in graduates is documented in the following five publications:

— *Education in Nuclear Science: A Status Report and Recommendations for the Beginning of the 21st Century,* DOE/NSF Nuclear Science Advisory Committee, Subcommittee on Education, November 2004.

— *Report to the Nuclear Science Advisory Committee: Guidance for Implementing the 2002 Long Range Plan,* 23 June 2005, pgs. 69–73.

— *The Future of the Nuclear Workforce: The Government's Role,* Laura Beth Bienhoff, Washington Internships for Students of Engineering, American Nuclear Society, 2003, 50 pgs.

— *Nuclear's Human Element: Defining the Federal Government's Role in Sustaining a Vibrant U.S. University-Based Nuclear Science and Engineering Education System for the 21st Century,* American Nuclear Society, Special Committee on Federal Investment in Nuclear Education, December 2006, 28 pgs.

— *Opportunities in Nuclear Science: A Long-Range Plan for the Next Decade,* DOE/NSF Nuclear Science Advisory Committee, April 2002, 148 pgs.

Risk Assessment

Q3. What sort of risk assessment does DNDO use when determining where to deploy their detection technology?

We heard in the hearing from you and Mr. Czerwinski that DNDO has global responsibilities; however it seems that deployment of detection technologies is limited to highly-visible, highly-trafficked ports of entry with relatively little attention given to intercepting smuggled materials in foreign countries or detecting materials smuggled across more remote borders. How do you decide where to direct your efforts?

A3. In assessing risks, DNDO relies on its gap analysis to guide the deployment of detection technology as well as the development of new detection technologies and new detection concepts of operation. In this analysis, DNDO has determined the existing baseline architecture of USG capabilities and organized it into a set of detection layers that are grouped into three main categories (international, border, and interior).

From this baseline architecture, DNDO looks at all possible paths from the original source of the radiological or nuclear material or weapon to a target within the U.S. Typically, DNDO will look at authorized pathways, e.g., Ports of Entry (POEs); other land, air, and maritime pathways; and unauthorized pathways (e.g., illegal crossing of land borders in remote areas). From this examination of pathways, DNDO identifies gaps, i.e., areas where detection is not currently sufficient. For each gap, DNDO identifies options to fill the gaps, evaluates the likely effectiveness of the options, and makes recommendations for programs (either deployment, new concepts of operations, or new research and development) to address the architecture gaps.

In formulating recommendations, DNDO is guided by the language in NSPD–43/HSPD–14, which states that "DNDO will be responsible for the implementation of the domestic portion of the global architecture," while "the Secretaries of State, Defense and Energy will maintain their respective responsibilities for policy guidance and implementation of the portion of the global architecture outside the United States." Those international responsibilities include State's EXBS programs, Energy's Second Line of Defense and Megaports programs, and Defense's Cooperative Threat Reduction activities. This process has led DNDO to focus additional efforts to develop detection strategies for general aviation pathways, small maritime pathways, and remote border crossings, as well as interior layer detection (e.g., Securing the Cities).

DNDO is constantly updating its gap analysis and, to the greatest extent possible, incorporating risk as it relates to the current threat as a factor in its deployment decisions throughout all (land, air, and maritime) pathways.

Questions submitted by Representative Phil Gingrey

Funding

Q1. Your testimony submitted to the Committee describes a remarkable difference in funding awards between National Laboratories and private industry and academia. For instance, you cite a call for proposals to National Labs in December 2005 that awarded nearly $40 million to 44 proposals from a pool of 150, a success rate of nearly 30 percent. Whereas, a similar announcement to the private sector and academia awarded only $3.1 million to seven institutions, out of a pool of 200 submissions: a 3.5 percent success rate.

What accounts for this stark difference in funding amounts and success?

A1. DNDO would like to clarify that the 200 submissions referred to above pertain to the informal white paper phase. The actual number of proposals received by private industry and universities was 75. Therefore, the number that should be compared to the 150 proposals for the National Labs is 75 rather than 200.

It should be further noted that DNDO made the awards in two parts. DNDO awarded the first set of grants to seven academic institutions, and the second set to 10 private industry participants. Thus, a total of 17 awards worth approximately $12 million have been made, putting the success rate at nearly 23 percent so far for this announcement.

The differences in award timing were due to differences in the grants and contracting processes. Regardless, these research projects were started as soon as the awards could be made. For FY 2007, awards to industry and academia will utilize approximately one-third of exploratory research funding under DNDO's Transformational Research and Development Directorate. Also, it should be noted that in addition to these projects, industry and academia have other projects and opportunities which are not included in the awards above. These include opportunities with DNDO's Small Business Innovative Research program and the newly initiated Academic Research Initiative.

Coordination Activities

Q2. At the hearing, you identified ways in which DNDO coordinates radiological detection research with other agencies and groups. Similarly, Under Secretary Cohen identified coordination activities undertaken by the S&T Directorate in his testimony. However, neither of your statements mentions coordination activities between DNDO and the S&T Directorate.

Do you consult with the S&T Directorate for strategic planning and budgeting purposes? What mechanisms exist within the Department of Homeland Security to coordinate and balance the activities of the S&T Directorate and DNDO? What interagency efforts are underway to plan across disciplines and threats?

A2. Yes. S&T and DNDO continue to have a close relationship within the Department, coordinating efforts at all levels—from the shared use of the radiological and nuclear expertise at the Environmental Measurements Laboratory (EML) to the integration of requirements and system development of technologies being developed for use in Departmental initiatives such as Secure Freight. In addition, there are multiple working level interactions that incorporate requirements and de-conflict overlapping and collocated sensor and architecture development programs. DNDO was also invited to participate in the S&T Integrated Product Team (IPT) process to provide them with out-year program insight and a sense of Departmental priorities in the R&D arena. Section 502 (d) of the *SAFE Port Act of 2006* also requires that S&T and DNDO develop an annual report that speaks to the coordination between the two Components.

Threats

Q3. Dr. Epstein suggests that improving methodologies for determining which threats to address and how much to spend on each should be a high priority for the government.

What activities do you have in your organization to address the need for decision-support and long-term strategic planning? What interagency efforts are underway to plan across disciplines and threats?

A3. DNDO recognizes the need for formal systems engineering processes to support and document mission, requirements, concepts of operation, and program perform-

ance. These processes include risk analysis to prioritize threats and cost-benefit analysis to evaluate particular programs.

Currently, DNDO is developing an end-to-end technology development plan that starts from a detection architecture gap analysis and documents the process from the identification of options, through prototype development, operational testing, deployment, and continuous evaluation. This documentation will provide decision support to the strategic planning process and will ensure the government pursues effective programs at every stage.

DNDO Red Teaming and Net Assessments (RTNA) are also developing an end-to-end probabilistic methodology for analysis of detection architecture effectiveness that is grounded in both adversary capability and detection node operational performance. Collaboration is occurring with Defense Threat Reduction Agency, elements of the intelligence community, Department of Energy, and United States Coast Guard on this project. This methodology will enhance global situational awareness and support interagency collaborative planning, course-of-action evaluations, tabletop exercises, including red team and blue team assessments, and analyses of battle management, exercise support, crisis action planning, and interagency collaborative planning. This will also be an effective tool to support technology investments and related decision making. The methodology defines and measures adversary capabilities through intelligent overlay of interagency threat databases, individual expert analyses, and adversary emulation operations. It also defines and measures detection node performance through network models for systems and CONOPS at individual detection layers and is based on a process developed for DNDO architecture studies and risk analyses.

In addition to DNDO internal risk assessment, DNDO is actively participating in DHS-wide programs such as the Risk Informed Planning Program which seeks to perform risk analysis across disciplines and threats to provide a comparable risk assessment between DHS components. DNDO is beginning to work directly with DHS Science and Technology to perform a WMD risk assessment common to chemical, biological, radiological, and nuclear weapons.

DNDO plays a key role in interdisciplinary planning. One of DNDO's founding principles was the allocation of responsibilities called, "centralized planning with decentralized execution." This means that DNDO is responsible for developing the global detection architecture, conducting test and evaluation of available systems that may be deployed, and assessing the effectiveness of the deployed architecture through red teaming and other means. However, it remains the responsibility of interagency partners to execute their respective portions of the global architecture.

Through centralized planning, DNDO seeks to fully utilize expertise from implementing agencies, and leverage, not duplicate, existing initiatives related to nuclear detection. Several mechanisms facilitate collaboration between interagency partners. For example, DNDO uses the Interagency Coordination Council (ICC) as a forum for effective coordination and, when required, as a mechanism for conflict resolution across all appropriate departments and agencies. ICC members will resolve policy issues that arise across organizational boundaries. In addition, members will serve as liaisons between their respective organizations and the DNDO to ensure that the interagency community is fully aware of each other's activities as they relate to the mission of the DNDO. Another example would be the use of interagency detailees as full-time DNDO staff members. These detailees play a critical role in helping DNDO interface with its implementing partners across the global nuclear detection architecture. Frequent dialogue facilitated by DNDO detailees with their home organizations results in a thorough understanding of implementing agency operations, technological requirements, reporting and information analysis needs—all of which drive DNDO operations.

Overview

Q4. Please provide to the Committee an overview of the activities DNDO has taken to include first-responders in the planning and operations of your research and development activities.

A4. To periodically engage the State and local (S&L) community, DNDO formed an S&L Stakeholder Working Group and has held five Working Group meetings each lasting three days. Working group meetings are designed specifically to bring the Nation's preventive rad/nuc detection community together, inform participants on activities within DNDO and the community, and obtain feedback on DNDO's programs and initiatives.

Since its inception, DNDO has made it a fundamental priority to work together with, and receive feedback from, its S&L first responders in developing programs and products. This continual loop of information exchange has been mutually bene-

ficial to DNDO and S&L jurisdictions and has helped refine various programs/products/services throughout the entire life cycle of the development process:

— Securing The Cities Initiative (STC): Under STC, DNDO has led a consortium of S&L stakeholders in the New York City region to establish a region-wide coordinated radiation detection and interdiction capability. This effort includes agencies from the States of NY, NJ, and CT. An overarching STC Working Group was established in January 2007, with several specialized committees including the Equipment Working Group. Through interactive discussions and live technology demonstrations, this group has addressed responder operational equipment requirements in an effort to focus DNDO acquisition and research efforts, and has agreed upon an initial set of equipment to be procured and distributed to responders throughout the region. This group has also brought developers of DNDO's SUV-based mobile Advanced Spectroscopic Portal System face to face with the operators in the region to facilitate the design process. Additionally, the group is addressing long-term sustainability issues such as equipment maintenance and calibration on a regional basis.

— Southeast Transportation Corridor Pilot (SETCP): Under SETCP, DNDO has reached out to nine Southeast States, plus the District of Columbia, and identified first responders with preventive rad/nuc detection responsibilities in their respective jurisdictions. For the last year, DNDO has met with these individuals at least quarterly and has solicited their functional requirements through directed surveys, interactive discussions, and live technology demonstrations. This group was instrumental in developing the Commercial Vehicle Inspection annex to the Preventive Rad/Nuc Detection Program Management Handbook. S&L participants also had input on the development of the functional requirements for the SUV-based mobile Advanced Spectroscopic Portal System. The SETCP live technology demonstration (November 2006) was operated entirely by S&L responders.

— Radiation Detection Device Testing: DNDO works closely with a group of S&L first responders to produce test results that would be helpful for S&L jurisdictions as they make decisions about which detection equipment to purchase. For the Anole test series, S&L first responders reviewed the draft report to ensure its readability and usefulness. For the Bobcat test series, CONOPS from S&L first responders were utilized to generate real-world test scenarios. Additionally, S&L first responders participated in hands-on testing of equipment.

— Display and Algorithm Integrated Product Teams (IPT): The Human Portable Radiation Detection System program staff, and the Human Factors Team that supported the Display and Algorithm IPTs, worked with S&L public safety representatives to help design equipment that would meet the needs of the first responders. Some of the entities who participated included: fire departments, law enforcement, and emergency management from Montgomery County, MD, Virginia Department of Emergency Management, and the Government of the District of Columbia. Additionally, the Human Factors Team coordinated its activities with other S&L public safety officials as well as with the U.S. Coast Guard, and Customs and Border Protection.

— Training Curriculum: DNDO worked with the S&L Stakeholder Working Group to review and gather training requirements, as well as develop curriculum for various levels and types of preventive rad/nuc detection training courses.

— Alarm Resolution Response Protocols: DNDO incorporated S&L public safety agencies into the development of detailed protocols for resolving detection alarms.

— Preventive Rad/Nuc Detection Program Management Handbook and Commercial Vehicle Inspection (CVI) Rad/Nuc Module: DNDO developed both of these products during numerous working sessions with a multi-jurisdictional, multi-disciplinary audience of S&L public safety officials. The program management handbook provides consistent guidance for building or enhancing State and local preventive rad/nuc detection programs. The CVI Rad/Nuc Module provides guidance to S&L jurisdictions that may choose to incorporate preventive rad/nuc detection into their CVI program in a variety of ways, including within mobile weigh station operations, within CVI roadside inspection operations, or by using relocatable portal monitors on by-pass routes.

— Homeland Security Presidential Directive (HSPD–8): DNDO worked with the DHS Office of Grants and Training to ensure consistency between HSPD–8 guidance and DNDO programs, as well as coordinate the involvement of S&L public safety representatives.
— Maritime Pilot and a Maritime Test Bed: S&L public safety representatives are currently working with DNDO to define the pilot and testbed.

Questions submitted by Representative Judy Biggert

RDD

Q1a. How is DHS implementing plans to protect against radiological weapons and radiological dispersal devices?

How does DHS evaluate the Radiological Dispersal Device (RDD) threat? What studies have been done to analyze the potential damage and consequences of an RDD attack? How does DHS distinguish its mission and R&D program on RDDs from that of DOE, DTRA, the military services and the FBI? What plans and programs does DHS have to analyze, mitigate, and respond to the RDD threat? How would DHS determine the source of an RDD attack? What data bases exist to support this effort? Since such an attack would be different from an actual nuclear explosion, how do these data bases differ from data bases maintained to determine the characteristics of foreign nuclear weapons? (The specific answer would probably be classified but the general question is: Are the data bases the same or different?)

A1a. DHS/DNDO has a three tiered approach, closely coordinated with other agencies, to protect the Nation from RDD devices. This approach includes: 1) identifying the potential radiological materials that could be used as an effective RDD; 2) securing and/or eliminating these sources and; 3) pursuing ways to make the commercial devices that employ radioactive sources more tamper proof. Examples of DNDO initiatives are documented below:

— DNDO is working with federal partners (NRC, DOE), industry, and licensees in the United States to investigate vulnerabilities and identify solutions to reduce the risk of unauthorized access to the Cesium-137 sources found in irradiators used in medical and research facilities.
— DNDO is participating with the NRC, other federal agencies, and the Agreement States in setting the data requirements for the national source tracking system to improve the usefulness of the database for source security.
— DNDO is participating in an effort to promote the design and production of non-nuclear alternatives for industrial devices that currently use radioactive sources.
— DNDO serves as the DHS representative on the NRC-chaired, Radiation Source Protection and Security Task Force, also known as the Energy Policy Act Task Force. The Task Force is responsible for a continuing comprehensive review of the status of radioactive source security and for reporting periodically to Congress on that status.
— DNDO is participating with the NRC, other federal agencies, and the Agreement States in the Alternative Technologies subgroup, as part of the Energy Policy Act Task Force. This subgroup is investigating the feasibility of alternatives to the commercial use of certain higher risk radioactive sources.
— DNDO is participating with the NRC, other federal agencies, and the Agreement States Cesium Chloride subgroup, as part of the Energy Policy Act Task Force. This subgroup is investigating methods to reduce the RDD risk from this particular radioactive source.

Furthermore, DNDO is beginning engagements with six UASI Tier I Urban Areas, followed by the additional 39 UASI Tier II Urban Areas by the end of FY 2009, as part of an operational implementation and outreach strategy that aims to improve State and local capabilities to detect and interdict radiological and nuclear threats. Coordinated implementation support includes: initial engagements with senior leaders from the Department of Energy, CBP, and the FBI; enlistment of the FBI's Joint Terrorism Task Forces; formulation of initial preventive rad/nuc detection program plans; threat briefings; response and protocol development; and training and exercise options.

Q1b. How does DHS evaluate the Radiological Dispersal Device (RDD) threat? What studies have been done to analyze the potential damage and consequences of an RDD attack?

A1b. DHS and DNDO use a combination of intelligence community and official government sources, as well as our own assessments, to evaluate a range of radiological and nuclear threats, including those posed by RDDs. The RDD threat is evaluated from both a threat and vulnerability standpoint—how susceptible are we to this type of attack, and what can be done to detect and prevent the attack. Numerous studies, both classified and unclassified have been conducted (including several under DHS sponsorship at the National Labs) that have characterized in detail the significant potential damage and consequences that could result from an RDD attack.

Q1c. How does DHS distinguish its mission and R&D program on RDDs from that of DOE, DTRA, the military services and the FBI?

A1c. From an R&D perspective, there are three key agencies doing R&D for nuclear detection: DOE/NA–22 focuses on R&D to support non-proliferation, proliferation detection, and counter-terrorism; DOD/DTRA focuses on R&D to support international interdiction and response, and counter-proliferation; and DHS/DNDO focuses on R&D to support prevention of a domestic event. Specifically, DOE and DTRA assist in the securing and detection of illicit trafficking of sources from or within other nations, which reduce the risk of RDDs domestically. The FBI brings to bear the investigative and law enforcement databases and professional relationships that DNDO relies on to make asset deployment decisions for potential domestic RDD threats.

We routinely coordinate with all of these agencies for ongoing projects and new announcements. This allows each agency to leverage technology advancements gained from other investments and transition needed technologies to users more rapidly. In addition, close coordination prevents redundancy in these R&D programs.

With respect to R&D for DNDO's nuclear forensics mission, DNDO's National Technical Nuclear Forensics Center leads a centralized, formalized interagency coordination process that ensures agencies' R&D programs and initiatives are jointly planned and executed in a manner consistent with roles and missions defined in national policy guidance.

Q1d. What plans and programs does DHS have to analyze, mitigate, and respond to the RDD threat?

A1d. DHS plans and programs related to RDDs may be divided into prevention and detection, which DNDO concentrates on, and mitigation and response, which are addressed by other DHS components such as the Directorate for National Protection and Programs, the Federal Emergency Management Agency, and the Office of Health Affairs; these programs have recently been re-organized and realigned. A significant DHS-wide and interagency effort has gone into preparing for RDD events, including contingency planning for the National Planning Scenarios, one of which is an RDD. DHS analysis of the RDD threat is ongoing. The generic effects of different types of RDDs employed in urban areas have been modeled, with some U.S. city-specific data generated to develop possible RDD scenarios. The predominant part of DNDO's mission involves the detection and prevention of radiological and nuclear terrorist events prior to the event happening.

DHS recognizes that an RDD threat could emanate from within our borders, so we are also working to improve detection and interdiction capabilities within our domestic interior as part of a broader layered defense. While detection at POEs, including systems that screen containers at seaports, is an important part of the solution, we must also develop solutions for non-POE applications for maritime, aviation, and land modes, including next-generation human portable detection equipment and mobile standoff assets. For example, DNDO is making progress to replace personal radiation detectors (pagers) now held by first responders with equally compact and more accurate devices that can detect both gamma and neutron radiation and identify isotopes of RDDs.

To improve source security and decrease the availability of radioactive sources to our adversaries, DNDO is working with other USG agencies and with industry to further protect and account for radioactive sources. DNDO is working to eliminate the sources within the United States that could be used for RDDs and also working to track radioactive sources of concern (industrial and medical) for security and situational awareness purposes. As a part of an interagency effort, DNDO also works with international counterparts to help other countries prevent and detect radiological or nuclear threats closer to the source.

Finally, we must remain vigilant and build greater public awareness of "what to look for," pre-detonation signs of radiological or nuclear threat anomalies in neighborhoods, workplaces, and transportation corridors that could launch a coordinated response to stop the attack.

The modeling work that is part of our initial analysis of the RDD threat can also help in post-event mitigation. DNDO has worked to computer model the effects of an RDD detonated in an urban area, allowing us to understand the size and scope of the impact on the population. In the event of an actual RDD event, DNDO will be a source of radiological/nuclear technical expertise and will support FEMA, HHS and other federal agencies to mitigate the effects.

Q1e. How would DHS determine the source of an RDD attack? What data bases exist to support this effort? Since such an attack would be different from an actual nuclear explosion, how do these data bases differ from data bases maintained to determine the characteristics of foreign nuclear weapons? (The specific answer would probably be classified but the general question is—are the data bases the same or different?)

A1e. In formulating the response to these questions, it is understood that the "source of an RDD attack" refers to "who is responsible" and this includes as one input the "source of material." It is further understood that the nuclear forensics process is necessarily interagency, with respective roles and responsibilities defined by statutes and policy directives. As part of the interagency effort DNDO is responsible for developing a "pre-detonation materials forensic analysis capability in support of the lead federal agency. In most instances the FBI will be the LFA and will be responsible for leading the interagency attribution effort. The following response addresses each question in turn:

Q1f. How would DHS determine the source of an RDD attack?

A1f. As indicated DHS is not responsible for determining the source of an RDD attack. DHS is improving/developing a pre-detonation materials forensic analysis capability that will be used principally by the FBI in support of its overarching attribution efforts. In general however, the key forensic processes supporting attribution of an RDD attack are described below:

— Material evidence would be collected from the scene that would contain nuclear forensic signatures indicative of the material source and RDD design. Conventional law enforcement forensic samples related to the conventional (non-nuclear) explosion would also be collected.

— The evidence would be analyzed at laboratories that have been equipped to conduct both radiochemical analyses and traditional forensic examinations of contaminated evidence.

— Many databases housed in various federal agencies exist to support conventional law enforcement forensics. Regarding the radioactive material source, databases are developed for this type of application.

— Data from analyses of the radiological material will be interpreted by the appropriate laboratory and, as required, peer reviewed by a group of experts to help identify the source of the material. The material's source is one input that will be used to address the question of "who is responsible?" Other traditional forensics will be utilized, and all the technical information will be combined with law enforcement and intelligence information to help develop the case for attribution (i.e., all source information fusion).

Q1g. What data bases exist to support this effort?

A1g. The President directed the development of an integrated system of information from all sources concerning worldwide nuclear material holdings and their security status, the Nuclear Materials Information Program.

Q1h. Since such an attack would be different from an actual nuclear explosion, how do these data bases differ from data bases maintained to determine the characteristics of foreign nuclear weapons? (The specific answer would probably be classified but the general question is—are the data bases the same or different?)

A1h. Due to fundamental differences in device design and materials used, there are inherent differences between the data captured in databases of RDD and nuclear weapon characteristics. In general, an RDD is very different from a nuclear device that produces yield. Essentially, the RDD databases cover two types of materials: 1) radiological sources and 2) nuclear fuels. Radiological source information includes information concerning commercial, industrial, and government produced or owned

radiological sources, and the nuclear fuels information captures reactor fuels information from commercial power, research, and government reactors. For both types of materials, much of the data are derived from manufacturing information and includes isotopic and elemental information, material information on the cladding and other structures (as applicable), date of manufacture, intended use, etc. Foreign nuclear weapons characteristics databases do not address radiological sources or reactor fuels (and are highly classified). Therefore, the databases are inherently quite different.

Outreach and Support

Q2. How is DHS implementing its outreach and support of regional assets? How are priorities set for funding regional assets? How are regional programs coordinated across all of DHS? What is the schedule for providing support to all regions of the country?

A2. DNDO, through its Operations Support Directorate and Office of State & Local Affairs, reaches out to State and local authorities and helps them prioritize their demand for federal support capabilities as well as identify their requirements for the design, requirements, and deployment of detection systems within the United States. DNDO is beginning engagements with the six (6) UASI Tier I Urban Areas, followed by the additional 39 UASI Tier II Urban Areas into the domestic layer of the GNDA by the end of FY 2009.

Working closely with the DHS Office of Intelligence and Analysis, DNDO ensures that national level expertise is in place to support prompt alarm adjudication. Reachback capability gives the responder community access to National Laboratory expertise to analyze spectral data and determine if a threat is present. We have established procedures and connectivity to three regional reachback laboratories as well as the National Operations Center. We routinely drill and exercise reachback capabilities, and have the capability to adjudicate all domestically referred primary-level radiation detection alarms. DNDO also works to ensure that regional preventative rad/nuc detection programs are coordinated across all of DHS. Coordinated support includes: initial engagements with senior leaders from the Department of Energy, CBP, and the FBI; enlistment of the FBI's Joint Terrorism Task Forces; formulation of initial preventative rad/nuc detection program plans; threat briefings; response and protocol development; and training and exercise options.

Through the Southeast Transportation Corridor Pilot (SETCP), DNDO is laying the groundwork for how DHS can encourage individual states to look at preventive rad/nuc detection as a necessary mission, as well as how states can coordinate with each other to regionally address rad/nuc threats. SETCP works through Regional Task Teams, comprising of state representatives from the law enforcement, radiological health, and emergency planning/operations communities. Dialogue with these representatives was coordinated through the State Homeland Security Advisors, both individually within each state and collectively across the region. As a result, the participating states have shared goals, technical approaches, concepts of operation (CONOPS) and lessons learned. In addition, DNDO has solidified support through the administration of two sets of Cooperative Agreements that have placed new radiation detection systems into the hands of individual states, but with an overlay of regional CONOPS to improve the use of these devices and to establish connectivity to the DNDO Joint Analysis Center and to Regional Reachback centers (also established by DNDO).

The following Cooperative Agreement awards have been made to States participating in the DNDO Southeast Transportation Corridor Pilot (SETCP). A portion of these awards (GA, KY, SC, TN, and VA) were awarded 26 Sept 2006. The remainder (AL, DC, FL, MS, NC) are scheduled for award on or about 1 June 2007. NOTE: Virginia is scheduled to receive an additional equipment allocation in FY2007 (an ASP Variant L unit) under their original Cooperative Agreement.

These Cooperative Agreements comprise a combination of cash grants, equipment grants, and services (such as site design and installation of fixed portal hardware). Cash grants supported local purchase of detector hardware, plus travel and allowable personnel costs for participation in SETCP-sponsored training and exercises.

State	Cash Award	Equipment Award	Total Award
Alabama	$ 198,163.22	$ 220,000.00*	$ 418,163.22
District of Columbia	$ 111,717.00	$ 220,000.00*	$ 331,717.00
Florida	$ 166,803.00	$ 220,000.00*	$ 386,803.00
Georgia	$ 149,070.72	$ 629,333.33	$ 778,404.05
Kentucky	$ 425,900.00	$ -	$ 425,900.00
Mississippi	$ 115,823.93	$ 783,835.00	$ 899,658.93
North Carolina	$ 153,185.57	$ 783,835.00	$ 937,020.57
South Carolina	$ 274,722.00	$ 629,333.33	$ 904,055.33
Tennessee	$ 381,587.91	$ -	$ 381,587.91
Virginia	$ 67,308.75	$ 849,333.00*	$ 916,642.08

*Final hardware costs for ASP Variant L are pending. These above figures reflect original unit costs projected by the ASP bidders in the Fall of 2006 ($220k per system). Final unit costs are likely to be higher.

Under the SETCP, the States are also being supported by the development of Concepts of Operation (CONOPS) to guide the use of the issued equipment. Each State is also receiving assistance in establishing a data exchange capability for preventive rad/nuc detection data, both within the state and between the state and the DNDO Joint Analysis Center (JAC).

Under Securing the Cities Initiative (STC), DNDO has led a consortium of S&L stakeholders in the New York City region to establish a region-wide coordinated radiation detection and interdiction capability. This effort includes agencies from the states of NY, NJ, and CT. An overarching STC Working Group was established in January 2007, with several specialized committees including the Equipment Working Group. Through interactive discussions and live technology demonstrations, this group has addressed responder operational equipment requirements in an effort to focus DNDO acquisition and research efforts, and has agreed upon an initial set of equipment to be procured and distributed to responders throughout the region. This group has also brought developers of DNDO's SUV-based mobile Advanced Spectroscopic Portal System face-to-face with the operators in the region to facilitate the design process. Additionally, the group is addressing long-term sustainability issues such as equipment maintenance and calibration on a regional basis.

DNDO also has a strong working relationship with the DHS Office of Grants and Training (G&T), particularly regarding the development and delivery of preventative rad/nuc detection training courses. DNDO, in coordination with G&T, develops and executes training courses, table tops, and other exercises and operational drills to provide federal, State and local agencies with structure processes to refine and standardize their procedures for the management of issues related to detection, alarm adjudication, incident reporting, and control and security of radioactive materials. This year's plans include training for 1,200 law enforcement personnel and first responders. In FY 2008, DNDO has a goal of training 2,400 individuals. DNDO also worked with G&T to ensure consistency between HSPD–8 guidance and DNDO programs.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Gerald L. Epstein, Senior Fellow for Science and Security, Homeland Security Program, Center for Strategic and International Studies

Questions submitted by Chairman David Wu

Q1. You pointed out in your written testimony that classified biological research can result in suspicion of the S&T Directorate's intent, and suggest that allowing outside observers to help oversee classified biological research can help alleviate some of the suspicion. Is the biology community currently involved in helping oversee S&T's biological research? If so, has S&T been providing outside observers with adequate information and access? If not, what do you recommend should be done?

A1. At present I am not aware of a mechanism by which members of the non-governmental biology community have the opportunity to review the entire biological research program, or the entire set of classified biological research activities, within the Department of Homeland Security. However, there are a number of mechanisms through which member of the non-governmental biology community with appropriate security clearances have or could have the opportunity to review specific biological research activities, including classified ones, that are conducted or sponsored by DHS. Without claiming that this list is necessarily complete, these mechanisms include:

- *Review by panels of the National Academies (the National Academy of Sciences, the National Academy of Engineering, the Institute of Medicine, and/or the National Research Council)*

  Federal agencies including DHS often make use of the National Academies to review research or address technical issues involving their research programs. Academy panels have the ability to obtain security clearances for panel members to enable them to address classified research. One particularly relevant panel is the Standing Committee on Biodefense Analysis and Countermeasures, the principal function of which is "to coordinate studies requested by the National Biodefense Analysis and Countermeasures Center related to biodefense analysis in support of the Department of Homeland Security" [1] According to National Academies' staff supporting this panel, all members of this panel, which includes distinguished academic biological scientists, have been granted or have applied for security clearances at the SECRET level, and they have received classified briefings in the past on the subject of risk assessment. This panel is in a position to receive unclassified or classified briefings (at the SECRET level or lower) on specific research activities associated with the National Biodefense Analysis and Countermeasures Center (NBACC), although I do not believe that it has yet been asked to do so.[2] (Disclosure: Although I am not a member of this panel, I have participated in several of its meetings as an invited guest speaker, including briefings and discussions on assuring compliance with the Biological Weapons Convention.)
- *NBACC Scientific Advisory Committee*

  Late in 2006, DHS awarded a contract to the Battelle National Biodefense Institute to operate NBACC, and this contractor is still in the process of establishing some of its management structures. According to staff within the Department of Homeland Security S&T Directorate, to which NBACC reports, Battelle intends to create an outside scientific advisory panel, including academic and other non-governmental scientists, that will presumably will have some standing responsibility to review and oversee the NBACC scientific program, including its classified aspects.
- *External Reviews by Entities such as the JASONs.*

---

[1] The National Academies, web page on Committee on Biodefense Analysis and Countermeasures (*http://www7.nationalacademies.org/BAST/BAST_Biodefense_Analysis_Committee.html*)

[2] Among other things, NBACC will perform studies and laboratory experiments—including classified ones—to "fill in information gaps to better understand current and future biological threats, assess vulnerabilities, conduct risk assessments, and determine potential impacts in order to guide the development of countermeasures. . ." (Fact Sheet: National Biodefense Analysis and Countermeasures Center," February 24, 2005, *http://www.dhs.gov/xnews/releases/press_release_0627.shtm*). Given its role in understanding potential threats, NBACC activities—and in particular classified NBACC activities—are likely to be controversial with respect to treaty compliance.

Should the Department of Homeland Security so wish, it could ask for reviews of its activities, including classified activities, by independent entities such as the JASONs, a group of non-governmental, largely academic scientists with high security clearances who do analyses and studies for a wide range of government agencies, including agencies in the national security sector. Members of this group can review highly classified programs.

Although originally comprised almost exclusively of physicists and other physical scientists, the JASONs have been expanding their domain of expertise and now include three nationally known biologists. To take on any significant role in reviewing life science research, this complement of life sciences would have to be expanded considerably, but at least there is an initial life sciences capability today. I am not aware that the JASONs have been asked to review any of DHS' classified biological activities, and they would typically not serve in a standing oversight role, but (subject to available personnel) they could be enlisted for specific studies.

I believe that DHS is providing adequate information and access to external reviews it has asked for, but I do not believe that outside reviews are currently being done on a systematic or comprehensive basis. (The DHS S&T program does undergo regular program reviews by scientists and others who are within government but outside DHS, including some from agencies such as NIH that are outside the traditional national security community.) Recognizing that it may be quite difficult and time-consuming for an outside group to be briefed on, and to probe in depth, an entire research portfolio—a task that clearly depends on the size and scope of that research portfolio—I would recommend that DHS implement a process in which non-governmental scientists with appropriate security clearances have more regular and more systematic opportunity to review the suite of classified DHS biological research activities. I note that DHS is currently implementing a process by which its entire research portfolio—both unclassified and classified—is reviewed by senior Departmental officials to ensure compliance with laws, treaties, and policy. This is a tiered review in which activities that warrant higher scrutiny get it—and a similar "tiering" philosophy could be applied to external technical review to DHS as well.

Since government agencies other than the Department of Homeland Security might also conduct classified biological research activities, it is also important that government-wide activities are reviewed with respect to technical merit and treaty compliance, and such reviews gain credibility to the extent that they involve members of the non-governmental biology community (and other outside observers). My conversations with senior government officials in several different agencies assure me that they are aware of the importance of such reviews and are working to develop processes to facilitate them. I would like to highlight two relevant efforts here.

- **The Biological Sciences Experts Group (BSEG) of the National Counterproliferation Center**

  In response to the recommendation of the *Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction* that the Intelligence Community engage more effectively with life scientists outside of the U.S. government, the National Counterproliferation Center within the Office of the Director of National Intelligence has created a Biological Sciences Experts Group (BSEG). This group, on which I serve, consists of non-governmental members with expertise in a range of disciplines associated with the biological sciences. Its members serve strictly in an advisory capacity. and they have no standing responsibility to review or assess classified biological research. However, members are available to provide advice on specific scientific and technical activities relevant to the Intelligence Community's missions, and they do constitute a mechanism to provide selected IC activities (which could include biological research) with independent, external, technical review. Speaking for myself, I believe it would be appropriate for BSEG members to address the credibility, legitimacy, and technical merit of IC biological research activities. Moreover, I believe—and have no reason to think my colleagues disagree—that the IC staffers working with this group are genuinely interested in obtaining independent and non-governmental views, and that they take seriously the requests and conclusions of BSEG members.

- **Wider technical and programmatic engagement and peer review by security-cleared non-governmental experts**

  Allowing more U.S. classified biological research activities to undergo external technical reviews would require increasing the availability of external reviewers who have security clearances. In the spirit of the *WMD Commission*'s

charge to the Intelligence Community to increase its engagement with the U.S. biological research community, efforts are underway to identify precisely these people—technical experts outside of government who currently hold security clearances—to ask them if they would be willing, on occasion, to perform technical reviews of classified projects.

Question submitted by Representative Phil Gingrey

Q1. How does the difference in structure between the end-to-end, research to operations, responsibilities of DNDO and the research-only management activities of the S&T Directorate affect their ability to provide technologies that reflect mature operational concepts and systems design?

A1. The difference in structure would likely complicate future efforts to merge DNDO with the S&T Directorate, but I don't see that it necessarily makes either of these organizations better in general at reflecting mature operational concepts and systems designs than the other.

Even though DNDO's role extends further "downstream" than S&T's does in terms of developing the architecture in which its products will be used, neither DNDO nor S&T is likely to be the employer of the individual who will be using that piece of equipment at the field. Both of these agencies, therefore, must overcome the difficulty of designing equipment for someone who is ultimately not under the agencies' direct control, and to which that agency might not have direct access.

DNDO has the explicit charge of developing an architecture for nuclear detection in addition to developing and procuring nuclear detectors themselves, whereas other DHS S&T activities seek to develop and deploy technology to support concepts, architectures, or requirements that are either in place already or are being developed by other DHS offices. (Biowatch had been an exception to this when its system architecture as well as its individual detectors were developed by DHS S&T, but responsibility for the overall architecture and operation of that program has since been moved out of DHS S&T.) In this sense, DNDO may have greater freedom to design systems and sensors that complement each other than DHS S&T, since it would presumably have fewer external constituencies or agencies to deal with. However, this does not necessarily mean that a DNDO system will better reflect "mature operational concepts," and could in fact imply the opposite: if DNDO does not have to meet requirements as established by another agency, it may be more tempted to set its own aggressive technical milestones that draw on less mature operational concepts. However, I am not aware of any specific evidence to that effect, and I am not sure this effect is very strong in any event.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Jonah J. Czerwinski, Managing Consultant, IBM Global Business Services; Senior Fellow, Homeland Security, IBM Global Leadership Initiative

Questions submitted by Chairman David Wu

Q1. In your opinion, what are the benefits of the Domestic Nuclear Detection Office's Securing the Cities Initiative? Is this type of project likely to be successful in preventing the unlawful transport and detonation of nuclear or radiological devices in the U.S.? Do you believe that the requested funding level of $30 million for FY 2008 is appropriate?

A1. The DNDO's Securing the Cities Initiative (SCI) reflects an investment in an important part of a layered defense. While efforts to secure sources of nuclear material in troubled areas remain critical, in addition to interdiction operations like the Proliferation Security Initiative, efforts like SCI help close an important gap in today's detection mission.

Because even the most effective global effort to stop illicit movement of dangerous nuclear material will be less than 100 percent successful, it is wise to consider domestic detection efforts in major cities. A perpetrator may be able to obtain nuclear material and evade detection overseas, en route, and across the U.S. border which is known to be porous in parts. If this occurs, it is likely that intelligence communities will have some warning and be able to provide law enforcement and other authorities with valuable information to aid in an apprehension. An SCI effort would greatly help augment intelligence and law enforcement officials by providing added warning and more accurate information about the location of nuclear material.

The scenario of nuclear material smuggled across U.S. borders, while dangerously possible, is perhaps as likely as nuclear material obtained from within the United States for use against a major U.S. city. Dangerous source material for a dirty bomb can be found in unsecured commercial locations or universities where nuclear material is located for legitimate uses. If a perpetrator steals this material, SCI capabilities provide a better ability to locate and isolate the material.

Whether or not SCI will be successful is difficult to say at this stage, but some precedence already exists that indicates such an effort could indeed be effective. The Department of Defense (DOD) already deploys their own version of SCI focused exclusively on protecting bases within the U.S. Detectors are in place surrounding the bases to detect a potential nuclear threat in vicinity of the base. Ongoing R&D for these programs is focused on increasing the ability to detect source material moving at greater speeds along public roads that lead to these bases. The potential for cooperation between DNDO and DOD should be pursued for mutual benefit.

Lastly, DNDO's budget request for SCI deserves attention. The Nation's investment in SCI should reflect a commitment to thinking creatively and responsibly about the threat of nuclear terrorism in America's cities. The nearly $11 billion to be spent on missile defense next fiscal year places the SCI budget in perspective. With an overall DNDO budget of approximately $550 million, dedicating $30 million to Securing the Cities seems appropriate. At this early stage, a healthier investment like this would help identify more promising routes to success while weeding out potential dead-ends. SCI is equal parts R&D and strategy.

Q2. From the FY 2008 budget request and information I've received from DNDO, it seems that deployment of detection technologies is limited to highly-visible, highly-trafficked ports of entry with relatively little attention given to intercepting smuggled materials in foreign countries or detecting materials smuggled across more remote borders. Is this an appropriate way to deploy detection technologies? If not, what factors should DNDO consider when determining where to deploy their detectors?

A2. The deployment strategy of detectors and other countermeasures in combating smuggling nuclear weapons may be one of the most important considerations in assessing the DNDO strategy. However, that the strategy and budget seem to indicate a focus on domestic choke points (i.e., highly trafficked points of entry) is appropriate at this stage for two reasons. First, efforts to detect or otherwise counter the threat of smuggled nuclear material overseas are mainly conducted by other agencies, but there is an important role for the DNDO. Second, the DNDO was wise to begin their deployment strategy at major points of entry first given the priority of closing obvious gaps soonest, but they must move forward with a plan to deploy

along less populated, and therefore less guarded, sections of the U.S. border, among other improvements.

The effort to combat smuggled nuclear material is a global one. Indeed the DNDO was originally named the National Nuclear Defense Office to reflect a broader mission than the one it is perceived to have today. After working its way through the interagency process, this title lost the word "national," which was replaced with Domestic, and the word "defense" became detection, in an apparent effort to winnow the mission of this new office. In practice, this makes some sense since both the Department of Energy and the Department of Defense also play a role in this area. The DHS office was given the detection mission only, but that has since evolved for good reason. Today, the DNDO works very closely with other agencies to develop not only new capabilities, but also the global deployment strategy that reflects and informs the use of detection efforts by all federal agencies including DOE, DOD, and others.

When the DNDO was created in April 2004, the White House placed significant emphasis on deploying detection capabilities quickly and in the most needed places. This had both positive and negative effects. The priority on deploying detectors quickly naturally sacrificed quality in the short run. The "pagers" and first-generation portal monitors (RPMs) suffered from poor selectivity that forced them to signal an alarm when encountering non-threatening materials that naturally contain radiation. This led to news reports and internal assessments that showed RPMs signaling a "hit" when only ceramic tile or other commercial material was found in an a container or truck hold. The other major trade-off that resulted from an accelerated deployment schedule was the low sensitivity of the earlier detectors (many of which are still in use). Low sensitivity leads many detectors to be unable to sense the presence of source material because, ironically, HEU and other elements actually give off very low levels of radiation prior to detonation. Current research and development underway at DNDO already shows major progress in both selectivity and sensitivity in a variety of settings.

The priority of placing detection capabilities at highly trafficked points of entry reflects a judgment call the DNDO and DHS leadership had to make at the time DNDO stood up and began using its first budget in FY 2005. Given limited resources, the constraints of a new organization, and an evolving threat, the choice was made to start with the most likely choke points based on traffic patterns (both licit and illicit) and the risk these areas posed to surrounding infrastructure and populations. Over time, the DNDO plan reflects an intention to contribute to antiterrorism programs overseas by supporting the DHS-DOE-State Department Secure Freight Initiative and NATO's Operation Active Endeavor. This is a positive development that also indicates the aggressive progress DNDO is making in the field of nuclear detection. Future development in DNDO's deployment strategy certainly includes efforts like Securing the Cities, but also networked detection capabilities in less traveled sections of the border to close those serious gaps you cited. An important improvement in strategy would include the use of decoys, hidden detectors, and mobile sensors to offset the adversary and increase the deterrent value of our antiterrorism capabilities.

Question submitted by Representative Phil Gingrey

Q1. How does the difference in structure between the end-to-end, research to operations, responsibilities of DNDO and the research-only management activities of the S&T Directorate affect their ability to provide technologies that reflect mature operational concepts and systems design?

A1. Improving technology, including better sensors and more effective forensics capabilities, is a vital—perhaps the most vital—step toward defending against a covert nuclear attack. To obtain this objective requires long-term, sustained research commitments across the Executive Branch and better use of the national labs, among other measures. While the lethality of a nuclear attack on the homeland is known among experts and decision-makers, a strategic approach to developing advanced sensing and detecting capabilities had become stove-piped and stultified in the Executive Branch prior to establishing the Domestic Nuclear Detection Office.

Acknowledging that the nuclear threat is different from most other threats posed by weapons of mass destruction, and that the expensive and complicated basic research needed to make progress is spread across several concerned agencies, including DHS, DOD, DOE, and others, this information served as the foundation for creating a single organization to draw upon existing capabilities and support development and acquisition of needed capabilities. To accomplish this critical mission, that

new organization required an end-to-end process that spans the effort from research to deployment.

Operations, however, were never presumed to be a part of the DNDO. To this day, the DNDO remains focused on research, development, and acquisition to support the originally stated mission of integrating and accelerating a better defense against smuggled nuclear weapons. Its charter stops short of an operational role, which should continue to be the responsibility of relevant authorities such as Customs and Border Protection and parts of the Defense and Energy Departments.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Marilyn Ward, Executive Director, National Public Safety Telecommunications Council (NPSTC)

Question submitted by Chairman David Wu

Q1. During the hearing, both Under Secretary Cohen and Director Oxford noted that the Department of Homeland Security Science and Technology Directorate and Domestic Nuclear Detection Office have efforts underway to respond to the needs of first responders. From the perspective of NPSTC and its members, how responsive has DNDO been to criticism of the high cost and difficulty of use of its technologies?

A1. The National Public Safety Telecommunications Council is focused on the issues of public safety wireless communications and inter-operability and does not closely follow or monitor the efforts of the Domestic Nuclear Detection Office. As such, I cannot comment on the responsiveness of the DNDO or its technologies.

Question submitted by Representative Phil Gingrey

Q1. What is the awareness of the TechSolutions website within the first-responder community? Will this site allow first-responders an appropriate level of access to DHS research and development planning?

A1. To the best of my knowledge, I am unaware that the National Public Safety Telecommunications Council community is aware of the TechSolutions website.

○