AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

NEXT GENERATION BORDER AND MARITIME SECURITY TECHNOLOGIES: H.R. 3916

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION

COMMITTEE ON SCIENCE AND TECHNOLOGY

HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

NOVEMBER 15, 2007

Serial No. 110–73

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

38–771PS WASHINGTON : 2008

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) 512–2104 Mail: Stop IDCC, 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
LAURA RICHARDSON, California
PAUL KANJORSKI, Pennsylvania
DARLENE HOOLEY, Oregon
STEVEN R. ROTHMAN, New Jersey
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
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
DAVID G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
MARIO DIAZ-BALART, Florida
PHIL GINGREY, Georgia
BRIAN P. BILBRAY, California
ADRIAN SMITH, Nebraska
PAUL C. BROUN, Georgia

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
LAURA RICHARDSON, California
BART GORDON, Tennessee

PHIL GINGREY, Georgia
VERNON J. EHLERS, Michigan
JUDY BIGGERT, Illinois
ADRIAN SMITH, Nebraska
PAUL C. BROUN, Georgia

RALPH M. HALL, Texas

MIKE QUEAR *Subcommittee Staff Director*
RACHEL JAGODA BRUNETTE *Democratic Professional Staff Member*
COLIN MCCORMICK *Democratic Professional Staff Member*
TIND SHEPPER RYEN *Republican Professional Staff Member*
PIPER LARGENT *Republican Professional Staff Member*
MEGHAN HOUSEWRIGHT *Research Assistant*

CONTENTS

November 15, 2007

	Page
Witness List	2
Hearing Charter	3

Opening Statements

Statement by Representative Bart Gordon, Chairman, Committee on Science and Technology, U.S. House of Representatives	8
Written Statement	9
Statement by Representative Ralph M. Hall, Ranking Minority Member, Committee on Science and Technology, U.S. House of Representatives	10
Written Statement	11
Prepared Statement by Representative David Wu, Chairman, Subcommittee on Technology and Innovation, Committee on Science and Technology, U.S. House of Representatives	12
Statement by Representative Phil Gingrey, Ranking Minority Member, Subcommittee on Technology and Innovation, Committee on Science and Technology, U.S. House of Representatives	9
Written Statement	9
Statement by Representative Harry E. Mitchell, Member, Subcommittee on Technology and Innovation, Committee on Science and Technology, U.S. House of Representatives	13

Witnesses:

Mr. Robert R. Hooks, Director of Transition, Science and Technology Directorate, Department of Homeland Security	
Oral Statement	14
Written Statement	17
Biography	20
Mr. Ervin Kapos, Director, Operations Analysis, Science and Technology Directorate, Department of Homeland Security; Executive Director, Homeland Security Science and Technology Advisory Committee (HSSTAC)	
Oral Statement	21
Written Statement	22
Biography	22
Dr. Brian A. Jackson, Associate Director, Homeland Security Research Program, The RAND Corporation	
Oral Statement	24
Written Statement	26
Biography	32
Chief Jeff Self, Division Chief, U.S. Border Patrol	
Oral Statement	32
Written Statement	34
Discussion	36

Appendix 1: Answers to Post-Hearing Questions

Mr. Robert R. Hooks, Director of Transition, Science and Technology Directorate, Department of Homeland Security	46

Page

Mr. Ervin Kapos, Director, Operations Analysis, Science and Technology Directorate, Department of Homeland Security; Executive Director, Homeland Security Science and Technology Advisory Committee (HSSTAC) 52

Dr. Brian A. Jackson, Associate Director, Homeland Security Research Program, The RAND Corporation 53

Chief Jeff Self, Division Chief, U.S. Border Patrol 55

Appendix 2: Additional Material for the Record

H.R. 3916, *To provide for the next generation of border and maritime security technologies* 60

NEXT GENERATION BORDER AND MARITIME SECURITY TECHNOLOGIES: H.R. 3916

THURSDAY, NOVEMBER 15, 2007

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

The Subcommittee met, pursuant to call, at 10:10 a.m., in Room 2318 of the Rayburn House Office Building, Hon. Bart Gordon (Chairman of the Committee) presiding.

The Subcommittee on Technology and Innovation

Hearing on:

Next Generation Border and Maritime Security Technologies: HR 3916

November 15, 2007
10:00 a.m. – 12:00 p.m.
2318 Rayburn House Office Building
Washington D.C.

WITNESS LIST

Mr. Robert Hooks
Director of Transition
Science and Technology Directorate, Department of Homeland Security

Mr. Ervin Kapos
Director of Operations Analysis
Science and Technology Directorate, Department of Homeland Security
Executive director
Homeland Security Science and Technology Advisory Committee (HSSTAC)

Dr. Brian Jackson
Associate Director, Homeland Security Research Program
RAND Corporation

Chief Jeff Self
Division Chief
U.S. Border Patrol

HEARING CHARTER

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

Next Generation Border and Maritime Security Technologies: H.R. 3916

THURSDAY, NOVEMBER 15, 2007
10:00 A.M.—12:00 P.M.
2318 RAYBURN HOUSE OFFICE BUILDING

1. Purpose

On Thursday, November 15, 2007, the Committee on Science and Technology's Subcommittee on Technology and Innovation will hold a hearing to discuss H.R. 3916 and examine the current and future priorities in border and maritime security research, development, and technology for the Department of Homeland Security's Science and Technology Directorate (DHS S&T).

2. Witnesses

Dr. Robert Hooks is the Director of Transition for the Department of Homeland Security's Science and Technology Directorate.

Mr. Ervin Kapos is the Director of Operations Analysis for the Department of Homeland Security's Science and Technology Directorate. He acts as the Executive Director of the Homeland Security Science and Technology Advisory Committee (HSSTAC).

Dr. Brian Jackson is an Associate Physical Scientist for the Science and Technology Policy Institute at the RAND Corporation.

Mr. Jeff Self is Division Chief of the U.S. Border Patrol.

3. Brief Overview

- The U.S. Customs and Border Protection (CBP) processes approximately 1.18 million people entering the United States through established ports of entry every day. CBP is also responsible for monitoring between legal entry points along the Northern and Southern borders and intercepting individuals attempting to cross the border. Border patrol officers also act as first responders, rescuing individuals in danger from extreme weather or violent situations at illegal entry points.
- Surveillance technology acts as a "force multiplier," which allows border patrol agents to augment their patrols with ground based and aerial observation capabilities. Examples of currently in-use security technologies include infrared sensors, automated cameras, and seismic sensors to detect motion, as well as air based observational equipment to monitor a large area.
- Many promising technologies are still not feasible for full implementation along the border because of numerous barriers: high cost, lack of robustness in harsh conditions, lack of personnel trained to properly use high-tech equipment, and technical problems. DHS S&T has primary responsibility for bringing new technologies to full readiness, with support from other agencies such as the National Institute of Standards and Technology, which provides testing and validation services.
- Additionally, many capability gaps, including situational awareness and officer safety, have been identified by end-users that require further basic and applied research to meet existing or anticipated challenges. DHS S&T has several mechanisms to receive advice on R&D priorities, including Integrated Product Teams (IPTs), which bring together stakeholders from other components of DHS, including CBP, in a regular, formal process to determine short-term technology needs. Advice on longer-term research priorities comes from

a number of sources, including the Homeland Security Science and Technology Advisory Committee (HSSTAC), the Homeland Security Institute (HSI), and the National Academies.

- The Border and Maritime Security Division of the DHS S&T Directorate has ongoing research projects focusing on advanced sensing capabilities, decision-making software tools, non-intrusive search capabilities, and other priorities. Additionally, the U.S. Coast Guard (USCG) and National Institute of Standards and Technology (NIST) carry out some border and maritime security technology research. USCG research includes officer protection, boarding, and suspect apprehension tools such as net guns for trapping fleeing boats. NIST has been conducting research on facial recognition technologies and fingerprint analysis, and technical tests of the RFID technology being incorporated into new electronic passports being issued by the State Department to prevent document counterfeiting.

4. Issues and Concerns

How does the DHS Science and Technology Directorate (DHS S&T) set overall research and development priorities? Under Secretary Jay Cohen, who took over leadership of DHS S&T in 2006, has established six research divisions that focus on specific technical areas. These divisions are Explosives, Chemical/Biological, Human Factors, Border/Maritime, Infrastructure/Geophysical, and Command, Control, and Inter-operability. Funding for each division is determined by the Under Secretary.

Short-term technology research priorities within each division are established by a formal mechanism based on a program at the Naval Research Laboratory (NRL). Integrated Product Teams (IPTs) bring together stakeholders from the mission components of DHS, such as the Transportation Security Administration (TSA) or Customs and Border Protection (CBP). The IPTs are organized by theme, and stakeholders first determine outstanding capability gaps and then rank research projects by order of urgency. Of the 11 IPTs, three deal with issues related to H.R. 3916: Border Security, Maritime Security, and Cargo Security.

Short-term projects determined through the IPT process account for roughly seventy percent of the DHS S&T budget and are managed by the Transition Portfolio Director. Longer-term basic research currently accounts for approximately thirteen percent with an announced goal of increasing this share to twenty percent over the next few years.

Currently, there is no strategic plan guiding longer-term research priorities. The agency turns to a number of resources for advice on long-term planning, including internal groups such as the Homeland Security Science and Technology Advisory Committee (HSSTAC) and the Homeland Security Institute (HSI) as well as outside think tanks and advisory bodies such as the National Academies. However, there is no mechanism to coordinate the efforts of the various advisory groups. The results of the efforts of these groups are unclear, however, as DHS S&T has not released a strategic plan outlining specific long-term research priorities.

TABLE 1: DHS S&T BUDGET

Budget category	FY 2006 Enacted [1]	FY 2007 Enacted	FY 2008 Request	FY 2008 House mark	FY 2008 Senate Mark	$ change/ request and House
Management and Administration	80.3	135.0	142.6	130.8	140.6	-11.6
Border and Maritime	**43.3**	**33.4**	**25.9**	**25.9**	**25.5**	**0**
Chemical and Biological	387.0	313.5	228.9	215.1	216.0	-13.8
Command, Control, and Interoperability	108.1	62.6	63.6	61.1	61.8	-2.5
Explosives	261.5	105.2	63.7	63.7	81.7	0
Human Factors	6.4	6.8	12.6	12.6	6.7	0
Infrastructure and Geophysical	86.1	74.8	24.0	24.0	64.0	0
Innovation	0	38.0	59.9	51.9	46.0	-8.0
Laboratory Facilities	83.2	105.6	88.8	88.8	103.8	0
Test, Evaluation, and Standards	34.6	25.4	25.5	28.5	24.2	+3.0
Transition	19.2	24.0	24.7	26.0	23.9	+1.3
University Programs	62.4	48.6	38.7	48.6	38.7	+9.9
TOTAL	**1487.0** [2]	**973.1**	**798.9**	**777.0**	**832.9**	**-21.9**

[1] Including 1 percent rescission.
[2] Includes funding for Domestic Nuclear Detection Office (DNDO) which received separate appropriations in FY 2007.

What are the current short- and long-term priorities in border and maritime security technology R&D? Is ongoing R&D helping to overcome some of the barriers to implementing specific border security technologies, such as unmanned aerial vehicles? Border and Maritime Security research is run through the Border and Maritime Division of DHS S&T, currently headed by Acting Director Captain Dave Newton (USCG). Additional border security research is carried out by other divisions within the S&T Directorate, most notably the Command, Control and Inter-operability (C2I) and Human Factors (HF) divisions as well as other agencies including the U.S. Coast Guard (USCG) and National Institute of Standards and Technology (NIST). Because of the many players in the border security technology realm, there are not consistent priorities across the many agencies and divisions. However, within DHS S&T, the divisions involved in border security research work to coordinate their efforts through the IPT process.

Currently, DHS S&T efforts are focused on situational awareness (the collection and harmonization of information about a situation from numerous sources), officer safety, and cargo security. The associated research projects span a variety of fields, including sensor technologies, command and control systems and software, connectivity tools, modeling and simulation, non-intrusive search tools, and cargo monitoring tools.

How will H.R. 3916 affect ongoing and future R&D at DHS S&T? H.R. 3916, introduced by Ranking Member Hall on October 22, 2007, strives to provide guidance to DHS S&T on the process of setting research priorities, ensuring that technology meets the needs of end-users, and on specific border security research priorities.

5. Background

This hearing will examine H.R. 3916, a bill introduced by Ranking Member Ralph Hall with the goal of improving long-term planning for research and development at the Department of Homeland Security, especially in the area of border and maritime security technology. The bill authorizes specific border security technology programs, and instructs DHS S&T to improve processes for setting research priorities and serving the needs of technology end-users.

Section-by-Section Discussion

Section 1: Requires the Department of Homeland Security Science and Technology Directorate (DHS S&T) to clearly define the operational requirements of technologies

they are developing for Customs and Border Patrol and other end-users. These one to three-year product development projects are part of the Transition portfolio at DHS S&T and comprise the bulk of research and development spending (approximately 70 percent).

This section is intended to ensure that both DHS S&T and the DHS customer component that will eventually own and operate the equipment developed have agreed to baseline requirements for operational as well as technical objectives. This requirement can be met through the Technology Transition Agreements (TTAs) that S&T currently negotiates for development work.

Section 2: Extends the S&T Advisory Committee, which was last extended through December 31st, 2008 in the SAFE Ports Act of 2006. *Currently S&T is appointing new members and has recently begun new meetings. The Committee briefly lapsed in November 2005. Further extends the Advisory Committee through December 31, 2012.*

The HSSTAC was created with the original *Homeland Security Act,* but lapsed once and has produced little for the Department. Since coming on-board last year, Under Secretary Cohen has reconstituted the committee and begun seeking their advice on specific topics. However, the committee will lapse again in December of 2008 without congressional action. The usefulness of the HSSTAC is largely determined by the Under Secretary's willingness to engage them in his decision-making, but letting them lapse would remove the only independent, S&T-focused advisory body immediately available to the department.

Section 3: Calls for an NRC study to provide a roadmap for research activities in the border/maritime division.

One of the primary gaps in DHS S&T's planning is the lack of a long-term research strategy. In 2002 the National Academies completed a 90-day study titled "Making the Nation Safer" that gave a general overview of how DHS S&T could support the then-fledgling Department. However, DHS S&T has failed to set specific long-term strategic priorities to guide research and development decisions. This section would allow the NAS to look specifically at one division of DHS S&T. The document produced by the NRC would give program managers at DHS a longer-term perspective than is provided through the one to three-year IPT process. If successful, similar reports could be commissioned for the other major DHS S&T divisions, such as Explosives or C2I.

Section 4: Reminds DHS of their role as a potential operator of Unmanned Aerial Vehicles (UAVs) in the national airspace and directs them to continue their work in the Joint Planning and Development Office accordingly. Currently, operation of UAVs in national airspace requires considerable advance planning and approval from the Federal Aviation Administration. Requires DHS to seek the ability to routinely and safely operate UAVs for border and maritime security missions. Authorizes DHS to take part in pilot projects to obtain whatever data is necessary to make an informed decision about how UAVs can be safely included in the airspace.

Several laws enacted in the 108th and 109th Congresses instructed DHS to work towards implementing a UAV surveillance program for border security. Numerous challenges have prevented DHS from launching a broad UAV program, including safety concerns. UAVs currently have an accident rate 100 times greater than that of manned aircraft. They are also more susceptible to adverse weather conditions than manned aircraft. These safety issues can likely be solved through further research, but flight tests will be an integral part of improving UAV technology. However, under current FAA regulations, UAVs cannot fly in the U.S. without special permission.

DHS is involved in an inter-agency planning group, the Joint Planning and Development Office (JPDO), to design the Nation's next generation air traffic control system, including UAV use. However, DHS's involvement to date is principally through the TSA. Given the high likelihood that DHS components would operate UAVs in the U.S., the Department should take a more active role now in planning for their introduction.

Section 5: Requires DHS to create a formal research program in the area of tunnel detection, and to coordinate with similar DOD activities. Calls for priority to be given to technologies that would allow real-time detection of tunnels and would allow for immediate action by Customs and Border Protection (CBP) officers.

Various advanced fencing and surveillance technologies are currently being tested as part of the Secure Border Initiative. However, in San Diego, where the double-

layer Sandia fencing has been constructed, smugglers have dug numerous tunnels underneath the border fence, including one concrete-reinforced, kilometer-long tunnel. This is just one example of the systemic challenges that face border patrol agents. With time and resources, committed individuals can avoid most border surveillance by simply digging right past them. Furthermore, detecting tunnels is remarkably difficult and solutions in the one to three-year time-frame are not likely. This has led DHS S&T and CBP to focus on other near-term priorities. This section asserts Congressional interest in a long-term tunnel detection program.

Section 6: Requires the Under Secretary for S&T and Director of NIST to begin a joint R&D project of anti-counterfeit technologies and standards. Furthermore, this designee is charged with coordinating research activities with other federal agencies engaged in related research. Requires a report to Congress on the research programs undertaken under this section one year after enactment.

Counterfeit documents are a major problem at legal ports of entry, with individuals attempting to enter the U.S. using fraudulent passports, identification, or birth certificates. CBP intercepts over 200 fake documents daily at the Nation's borders, but technology for creating counterfeit documents is growing increasingly sophisticated and fraud is increasingly difficult to detect. The Federal Government has begun to support research activities to development technology for verifying documents, but currently activity in this area is broadly distributed with DOD, Treasury, Immigrations and Customs Enforcement, State, and Justice all pursuing various aspects. DHS S&T, however, has not been actively involved despite the clear impact on agencies such at ICE and CBP.

Chairman GORDON. Good morning, everyone, to today's hearing on *Next Generation Border and Maritime Security Technologies.*

Now, the mission of U.S. Customs and Border Protection is one of the most difficult within the Department of Homeland Security. CBP officials are responsible for securing the movement of people and goods by air, land, sea, across our nation's borders. That job is part law enforcement, part first responder, part diplomat, and part detective, and the scope of CBP's job is enormous. Nearly 1.2 million people come through our legal ports of entry every day. In addition, illegal activity, including unlawful border crossing, drug smuggling, and human trafficking is persistent.

The State Department estimates that nearly 18,000 people are smuggled into the U.S. every year for the purpose of forced labor. They also report that nearly 90 percent of the cocaine and the majority of the heroin in the U.S. comes from our southern borders. It is clear that these agents need the help of new technology to do their jobs better, and to make our borders more secure.

Technology acts as additional eyes and ears for Border Patrol agents, allowing for observation of border areas 24 hours a day. The Department of Homeland Security's Science and Technology Directorate supports R&D to meet technology needs of the Department's components, including CBP. There are some promising technologies that have been deployed, but the enormous scope of the border security challenge requires a long-term strategic plan that has not yet been developed. Without a specific plan for border security technology research, long-term basic research will be disconnected from the real-life challenges of coming years and decades.

Additionally, short-term priorities must be more responsive to the needs of end-users. When he appeared before the Technology and Innovation Subcommittee in March, Under Secretary Cohen outlined measures that DHS S&T is taking to involve end-users in setting research priorities, including integrated product teams and Web-based means for soliciting end-user opinions on technical needs. But DHS must do more than simply identify capability gaps. End-users should be able to provide feedback on cost, robustness, and other characteristics that determine whether a technology will be adopted or whether it will sit on the shelf. This is especially true for border security technologies, which are often used by agents without significant technical training in harsh environments.

I would like to commend Ranking Member Hall on his bill, H.R. 3916, which takes important steps toward improving the capabilities of the Border Patrol to prevent criminal activities at and around our nation's borders. Mr. Hall's bill authorizes important programs to enhance Border Patrol's ability to carry out its mission by supporting short- and long-term research priorities. Additionally, it ensures that new technologies will be useful to Border Patrol agents by mandating that DHS work to meet cost and training needs of end-users when developing these technologies. This bill is a concrete step toward solving a complex issue now, on how to secure our nation's borders against those who would do us harm. I look forward to working with Ranking Member Hall on this bill as we move forward.

I now recognize Dr. Gingrey, the Ranking Member, for his opening statement.

[The prepared statement of Chairman Gordon follows:]

PREPARED STATEMENT OF CHAIRMAN BART GORDON

I'd like to thank Chairman Wu for calling today's hearing and commend Ranking Member Hall on his bill, which takes important steps towards improving the capabilities of the Border Patrol to prevent criminal activity at and around our nation's borders.

Border Patrol agents are responsible for securing nearly seven thousand miles of land borders to the North and South, as well as ninety-five thousand miles of shoreline. While our current corps of border patrol agents is doing a commendable job, their job is daunting.

Technology can play a vital role in extending observational capabilities, helping border patrol agents locate suspects and monitor the border more effectively.

Mr. Hall's bill authorizes important programs to enhance the border patrols ability to carry out its mission by supporting short- and long-term research priorities.

Additionally, it ensures that new technologies will be useful to border patrol agents by mandating that DHS work to meet cost and training needs of end-users when developing these technologies.

This bill is a concrete step towards solving a complex issue: how to secure our nation's borders against those who would do us harm.

I look forward to working with Ranking Member Hall on this bill as we move forward.

Mr. GINGREY. Good morning, Chairman Gordon, and I want to thank you for, of course, holding this hearing on H.R. 3916, the border security bill that was introduced by the distinguished Ranking Member of the Full Committee, Mr. Hall, of Texas.

As an original co-sponsor of H.R. 3916, I am pleased to see that the Science Committee and specifically this subcommittee, which I am Ranking Member of, the Subcommittee on Technology and Innovation, is taking an active role in securing our borders, and I believe it is one of the most important issues facing this Congress and the country as a whole.

Mr. Chairman, I commend both you and Chairman Wu for co-sponsoring the legislation that does improve long-term planning for R&D at the Department of Homeland Security and border and maritime security technology. As a Member of the Congressional Immigration Reform Caucus, I support and I have authored legislation that will help secure our borders and discourage illegal immigration. I believe that H.R. 3916 will assist the Department of Homeland Security and U.S. Customs and Border Protection Agency in long-term utilization of technologies to help us secure our border from threats that face our nation.

Mr. Chairman, I am indeed, as I say, proud to support this legislation, and at this time, I will yield back to you.

[The prepared statement of Mr. Gingrey follows:]

PREPARED STATEMENT OF REPRESENTATIVE PHIL GINGREY

Good Morning Chairman Wu. I want to first thank you for holding this hearing on H.R. 3916 the border security bill introduced by the distinguished Ranking Member of the Full Committee, Mr. Hall of Texas. As an original co-sponsor of H.R. 3916, I am pleased to see that the Science Committee—and specifically the Subcommittee on Technology and Innovation—is taking an active role in securing our borders, which I believe is one of the most important issues facing this Congress and our country as a whole.

Mr. Chairman, I commend both you and Chairman Gordon for co-sponsoring this legislation that improves long-term planning for R&D at the Department of Homeland Security in border and maritime security technology. As a Member of the Congressional Immigration Reform Caucus, I support and have authored legislation that will secure our borders and discourage illegal immigration. I believe that H.R. 3916 will assist the DHS and the U.S. Customs and Border Protection agency in

long-term utilization of technology to help us secure our border from threats that face our nation.

Mr. Chairman, I look forward to hearing today's testimony from our panel on this vital issue of border security and the solutions they have that will enable us to plan for the use of emerging technologies in the future. With that Mr. Chairman, I yield back.

Chairman GORDON. With no objections, I would like to yield to Mr. Hall for whatever time he might consume.

Mr. HALL. Mr. Chairman, thank you, and I join Dr. Gingrey in his accolades for your cooperation and assistance in holding a hearing on border security and House Bill 3916, that I introduced just a few weeks ago, and I think it is a crucial issue for the Committee to discuss, and I would like to thank you and the Full Committee, Chairman Gordon. I thank you personally for co-sponsoring this legislation and bringing this very capable panel before us today. I would also like to thank Mr. McCaul for the substantial contribution he made to the bill.

Border security is a concern of all Members of Congress, and we have nearly 7,500 miles of border, land border with Canada and Mexico, over which half a billion people and 2.5 million rail cars pass each year. In addition, we have over 300 ports that see over nine million cargo containers each year. Now, we have a myriad of reasons for wanting strict control over this traffic. For instance, according to Department of Justice statistics, over 30,000 kilograms of cocaine, heroin, and meth were seized within 150 miles of the U.S.-Mexico border in 2006.

I know many Members of this committee have worked tirelessly and hard to end the meth problems in our nation, yet success at restricting access to meth ingredients here in the States has led drug dealers to import more across our borders. Stopping the flow of narcotics across our borders remains, I think, key to our efforts to curb illegal drug use.

The threat of terrorism also compels us to re-examine our borders. Whether we are talking about foreign groups trying to infiltrate our country, or homegrown terrorists seeking weapons and supplies, our borders remain a critical element of our defenses. Our enemies, however, are adaptive and guileful. One of our witnesses today, Dr. Jackson, has tracked a number of terrorist groups and has sage advice about our need for a multi-layered defense.

Finally, in Fiscal Year 2005, U.S. Border Patrol agents apprehended 1.19 million people attempting to enter the country illegally. While I understand the concerns many Members have regarding comprehensive immigration reform, we should not allow that issue to stymie progress deterring terrorists, drug smugglers, and human traffickers.

I believe this committee is ideally positioned to strengthen control of our nation's borders through bipartisan legislation supporting effective, efficient, and evolving defenses. H.R. 3916 begins this effort. The sections in this bill reflect a single underlying theme. The Science and Technology Directorate at DHS needs to establish long-term goals and objectives for border security and broaden science and technology community involvement. The bill highlights three long-term research areas: unmanned aerial vehicles, tunnel detection, and anti-counterfeit technologies that prom-

ise to significantly improve border security across all the threats and against all the threats that we currently face.

I have a longer statement for the record that includes additional background on H.R. 3916, but in the interests of time, I will yield following one parting thought, and that is that border security is one of the most difficult problems faced by scientists and engineers. It is a complex system of—it is just a system of systems, that will require concerted interdisciplinary attention over many years, and I urge this committee to take the lead in Congress to push a long-term, adaptable, science-enabled border security policy.

And I yield back my time, and I thank the Chair.

[The prepared statement of Mr. Hall follows:]

PREPARED STATEMENT OF REPRESENTATIVE RALPH M. HALL

Chairman Wu, thank you for holding this hearing on border security and the bill H.R. 3916 that I introduced just a few weeks ago. I believe this is a crucial issue for this committee to discuss. And I would like to thank you and Full Committee Chairman Gordon for co-sponsoring this legislation and bringing this capable panel before us today. I'd also like to thank Mr. McCaul for the substantial contribution he made to the bill.

Border security is a concern of all Members of Congress. We have nearly 7,500 miles of land border with Canada and Mexico, over which half a billion people and 2.5 million rail cars pass per year. In addition we have over 300 ports that see over nine million cargo containers each year. Meanwhile, the Government Accountability Office estimates that one in ten serious drug and weapon violators and illegal immigrants pass through airports and land borders undetected.

We have a myriad of reasons for wanting strict control over this traffic. For instance, according to Department of Justice statistics, over 26,000 kilograms of marijuana were seized in northern border states in 2005 while over 30,000 kilograms of cocaine, heroine, and methamphetamine were seized within 150 miles of the U.S./Mexico border in 2006. Stopping the flow of narcotics across our border remains key to our efforts to curb illegal drug use. I know many Members of this committee have worked tirelessly to end the scourge of methamphetamine in our nation. Yet, success at restricting access to meth ingredients here in the States has led drug dealers to import more across our borders.

The threat of terrorism also compels us to re-examine our borders. Whether we're talking about foreign groups trying to infiltrate our country or home-grown terrorists seeking weapons and supplies, our borders remain a critical element of our defenses. Major efforts in this area are well underway. With the help of the Science and Technology Directorate, Customs and Border Protection has created a massive screening program to detect nuclear material that might be smuggled in via cargo containers. Our enemies, however, are adaptive and guileful. One of our witnesses today, Dr. Jackson, has tracked a number of terrorist groups and has sage advice about our need for a multi-layered defense.

Finally, in fiscal year 2005, U.S. Border Patrol agents apprehended 1.19 million people attempting to enter the country illegally. While I understand the concerns many Members have regarding comprehensive immigration reform, we should not allow that issue to stymie progress deterring terrorists, drug smugglers, and human traffickers.

I believe this committee is ideally positioned to strengthen control of our nation's borders through bipartisan legislation supporting effective, efficient, and evolving defenses. H.R. 3916 begins this effort. The sections in this bill reflect a single underlying theme: the Science and Technology Directorate at DHS needs to establish long-term goals and objectives for border security and broaden science and technology community involvement. The bill highlights three long-term research areas, unmanned aerial vehicles, tunnel detection, and anti-counterfeit technologies, that promise to significantly improve border security across all the threats we currently face.

Section 1 requires S&T to include cost and operational objectives in any near-term application development. This section is meant to ensure that both S&T and the DHS component that will eventually own and operate the equipment developed have agreed to baseline requirements for operational as well as technical objectives. This requirement can easily be met through the Technology Transfer Agreements (TTAs) that S&T currently negotiates for development work.

Section 2 extends the S&T Directorate's advisory committee through 2012. The HSSTAC was created with the original *Homeland Security Act,* but lapsed once in that time. Under Secretary Cohen has reconstituted the committee and begun seeking their advice on specific topics. However, the committee will lapse again in December of 2008 without Congressional action.

Section 3 specifically addresses long-term planning in the border security realm by tasking the National Research Council with a needs assessment and road-mapping request. In 2002 the National Academies completed a 90-day study titled "Making the Nation Safer" that gave a general overview of how S&T could support the fledgling DHS. This section would allow the NAS to look specifically at one sector of DHS S&T. The document produced by the NRC would give program managers at DHS a longer-term perspective than is provided through the one to three-year IPT planning process. If successful, similar reports could be commissioned for the other major DHS S&T divisions, such as Explosives, Chem/Bio, or Cyber Security.

Section 4 directs the Secretary of DHS to take an active role in safely incorporating unmanned aerial vehicles into the national airspace. UAV's cannot currently fly in the U.S. without special permission from the FAA. DHS is involved in an interagency planning group, the JPDO, to design the Nation's next generation air traffic control system, including UAV use. Given the high likelihood that DHS components would operate UAVs in the U.S., the Department should take a more active role now in planning for their introduction.

The tunnel detection program described in Section 5 aims at solving a persistent smuggling problem. Organized crime has the time and resources to avoid most border surveillance by simply digging right past them. However, detecting tunnels is remarkably difficult and solutions in the one to three-year timeframe are not likely.

Similarly Section 6 asserts Congressional interest in a sustained program to defeat counterfeiting. Activity in this area is broadly distributed in the Federal Government with DOD, Treasury, Immigrations and Customs Enforcement, State, and Justice all pursuing various aspects. DHS S&T, however, does not have a devoted office or program in this area despite the clear impact on agencies such at ICE and CBP.

Border security is one of the most difficult problems faced by scientists and engineers. It is a complex system of systems that will require concerted, interdisciplinary attention over many years. I urge this committee to take the lead in Congress to push a long-term, adaptable, science-enabled border security policy.

Chairman GORDON. Thank you, Mr. Hall. Your full remarks will be made a part of the record. As a Texan, you have first-hand knowledge of this, and I can assure you that the Majority looks very forward to working with you and Dr. Gingrey and your staff and other Members of this committee on this important issue. It will be fast tracked, and we will, again, be as accommodating as you would like.

[The prepared statement of Chairman Wu follows:]

PREPARED STATEMENT OF CHAIRMAN DAVID WU

I want to thank everyone for attending today's hearing on *Next Generation Border and Maritime Security Technologies.*

The mission of the U.S. Customs and Border Protection is one of the most difficult within the Department of Homeland Security. CBP officials are responsible for securing the movement of people and goods by air, land, and sea across our nation's borders. That job is part law enforcement, part first responder, part diplomat, and part detective. And the scope of its job is enormous. Nearly 1.2 million people come through legal ports of entry every day. In addition, illegal activity—including unlawful border crossings, drug smuggling, and human trafficking—is persistent. The State Department estimates that nearly 18 thousand people are smuggled into the U.S. every year for the purpose of forced labor. They also report that nearly 90 percent of cocaine and a majority of the heroin in the U.S. comes across our Southern border.

The House has voted to increase the number of Border Patrol officers by 3000, and it is clear that these agents need the help of new technology to do their jobs better and to make our borders more secure. Technology acts as additional eyes and ears for Border Patrol agents, allowing for observation of broad areas 24 hours a day. Innovative technologies such as unmanned aerial vehicles, infrared sensors, and motion detectors help border agents identify where illegal activity might be taking place, multiplying the effectiveness of existing and added CBP staff.

The Department of Homeland Security's Science and Technology Directorate supports R&D to meet the technology needs of the Department's components, including CBP. There are some promising technologies that have been deployed, but the enormous scope of the border security challenge requires a long-term strategic plan that has not yet been developed. Without a specific plan for border security technology research, long-term basic research will be disconnected from the real life challenges of coming years and decades.

Additionally, short-term priorities must be more responsive to the needs of end-users. When he appeared before this subcommittee in March, Under Secretary Cohen outlined measures that DHS S&T is taking to involve end-users in setting research priorities, including Integrated Product Teams and web-based means of soliciting opinions.

But DHS must do more than simply identify capability gaps that need to be filled with technology. End-users should be able to provide feedback on cost, robustness and other characteristics that determine whether a technology will be adopted or whether it will sit on the shelf. This is especially true for border security technologies, which are often used by agents without significant technical training in harsh environments.

I want to thank the Ranking Member of the Full Committee, Mr. Hall, for introducing H.R. 3916, which we will be discussing today. That legislation addresses these crucial issues and brings up some important questions. Do we have the technology we need to help CBP do its job? Do the new technologies developed by DHS meet the needs of end-users in terms of cost and ease of use, and other important parameters? And, more generally, how is the DHS Science and Technology Directorate determining priorities for R&D?

I'm eager to hear our witnesses' thoughts on the answers to these questions. I am especially interested to hear our DHS witnesses' comments on how they will work to meet the technology needs of the border patrol in the short- and long-term. We need to do a better job of aligning research to the needs of end-users, and I'm looking forward to working with my colleagues to promote innovative technology to support our nation's hardworking border patrol.

[The prepared statement of Mr. Mitchell follows:]

PREPARED STATEMENT OF REPRESENTATIVE HARRY E. MITCHELL

Border security is an issue that truly hits home. Illegal immigration affects Arizona more than any other state-more than half of illegal crossings over the U.S.–Mexico border happen in Arizona.

When the Federal Government fails to live up to its responsibility, Arizona pays a hefty price. Illegal immigration fosters violent drug and human smuggling crimes, and burdens our local law enforcement and emergency rooms.

These illegal crossings threaten our national security. We must do better.

We can start by ensuring that these border agents have all the tools necessary to protect our borders. Stopping people from crossing the border is not as simple as building a fence. These people sneak across the border daily by going to underpatrolled areas, jumping over fences, and building underground tunnels.

I am proud to co-sponsor Chairman Hall's legislation, H.R. 3916, which will help provide our border guards with technologically advanced equipment to monitor the borders. Significantly, this bill will improve border security by advancing technology for tunnel detection as well as aerial monitoring of the border.

I look forward to hearing from our witnesses on how this legislation will help secure our borders.

I yield back.

Chairman GORDON. Let me also say, this is a very distinguished panel. I want to thank you for taking your time to be here. We have Members that are in both parties, who have conferences and meetings this morning getting started, so we are going to have some folks coming in. This hearing is televised. Staff are watching it both from the anteroom and back in the offices, and Members are watching it there, too, so your testimony falls on a large audience, and we want to have that input from all.

So now let me introduce our distinguished panel. First, Mr. Robert Hooks is the Director of Transition at the Department of Homeland Security Science and Technology Directorate, also known as

DHS S&T. Mr. Ervin Kapos is the Director of Operations Analysis at the DHS S&T and coordinates the Homeland Security Science and Technology Advisory Committee, called HSSTAC. And Dr. Brian Jackson is the Associate Director of the Homeland Security Research Program at the RAND Corporation. And Mr. Jeff Self is the Division Chief for the U.S. Border Patrol, for some real-world information here today. Thank you, Chief, for being here.

And as our witnesses should know, the spoken testimony is, we try to limit it to five, but we don't want you to feel uncomfortable. If you—we really want your information, if you take what you need, and the remainder of your testimony will certainly be in the record.

And we will now start with Mr. Hooks.

STATEMENT OF MR. ROBERT R. HOOKS, DIRECTOR OF TRANSITION, SCIENCE AND TECHNOLOGY DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY

Mr. HOOKS. Good morning, Chairman Gordon, Ranking Members Hall and Gingrey, and distinguished Members of this subcommittee. I am Robert Hooks, and I should clarify, I am not a doctor. I wish I was, but I am not.

I am the Director of Transition Portfolio for the Science and Technology Directorate of the Department of Homeland Security, and I am pleased to appear before you today to discuss the successes that the Department of Homeland Security's Science and Technology Directorate have achieved with respect to technology solutions on our borders, both land and sea. Under Secretary Cohen asked me to express his appreciation and thanks to this committee, your staffs, and the entire Congress for the strong bipartisan leadership and support you have given him and the men and women of the Science and Technology Directorate as we work to make the Nation safer.

Nearly 14 months ago, with Congress' support, Under Secretary Cohen implemented a new organizational structure for the Science and Technology Directorate, to make it customer focused and output oriented. Our customers are the operating components and directorates of DHS, and their stakeholders are the State, local, tribal governments, first responders, and the private-sector entities. Our Science and Technology effort to deliver technology is primarily organized into three portfolios: transition, innovation, and basic research.

The Product Transition Portfolio, for which I am the Director, is centered on 11 functional DHS customer-led, Capstone Integrated Product Teams, three of which are Maritime Security, Cargo Security, and Border Security. In the Capstone IPTs, DHS operational components, and directorates are the chairs or co-chairs. They define and prioritize the capability gaps, then S&T offers technical solutions, where the customer is then the final approval on if the offered technical solution is appropriate for them.

While we have identified the principal customers within the Capstone IPTs, as the chairs or co-chairs, they are not the only representatives at these IPTs. All of the DHS operational components and directorates are invited as customers to any Capstone IPT relevant to their mission. As an example, because of the interrelation-

ship within their respective geographic areas of responsibility, Coast Guard has representation at the Borders IPT, and CBP is represented at the Border Security IPT.

Directed by the priorities of the Border, Cargo, and Maritime Security Capstone IPTs, S&T is developing technologies that can be delivered to components in the near-term, usually less than three years, to assist in securing our maritime land borders and protecting CBP and Coast Guard law enforcement officers, and you see some of those displayed on the placards and also at the table.

We are pursuing efforts to deliver advanced detection, identification, apprehension, and enforcement capabilities along land and maritime borders, and provide advanced technology, spiral development injections into DHS component program areas, such as SBInet, Command 21, the Secure Freight Initiative, Container Security Initiative, and Customs Trade Partnership Against Terrorism, CTPAT.

Specifically in the border security area, a number of our near-term product transition programs focus on developing detection, classification, and localization sensor technology to monitor illegal border activity with a wider range and greater accuracy than present-day technologies and command-and-control systems that deliver a much broader amount of information about current events to different levels of law enforcement, communication systems that provide connectivity for law enforcement officers working in remote locations, as well as modeling and simulation tools to help border enforcement agencies make informed improvements in immigration and border security policy and operations, and appropriate investments in technology, complex systems, and infrastructure. These technologies and systems will help to ensure that maritime and border security assets are used effectively and efficiently, and enable law enforcement to have access to robust and reliable intelligence when they need it.

S&T is also developing and delivering technologies that will enable border security and Coast Guard members to perform their current tasks more efficiently, effectively, and with a higher level of safety. Development of these tools, in many cases, is leveraged from the initial investment of other government agencies, such as the Department of Defense and the National Institutes of Justice, and then adapt it to fit the operational environment and functions of the several DHS security components.

We are also developing near-term technologies to improve supply chain security and thus decrease screening frequency and simultaneously increasing our probability of detection against dangerous contraband. Using a system-of-systems approach, we are developing advanced sensor and communication technologies within a security architecture that encompasses the world's supply chain. Some of the technologies developed in this program will enable CBP officers to identify tampering events, their location, track the shipping containers, and ensure that alarm data is communicated reliably and securely.

Consistent with H.R. 3916, we recognize that our technology effort needs to account for the affordability, life cycle costs, and the training costs. This way, if the procurement based on our new technology would be too expensive for the component or the operating

costs too prohibitive, the decision to look for a new technology solution can be made early, before large acquisition buy programs are initiated, and before the federal, State, local, and tribal entities expend their precious resources.

The basic research portfolio addresses long-term research and development needs in support of the DHS mission areas that will provide the Nation with an enduring capability in homeland security. The basic research program is focused on research projects that clearly contribute to the goals of S&T's DHS customers and is informed by the customer capability gaps identified in the Capstone IPTs.

This type of focused, long-term research investment has the potential to lead to paradigm shifts in the Nation's homeland security capabilities. An example is in tunnel detection. This is a type of long-term, focused research effort that would be tackled in the basic research area. As you are probably aware, the threats posed by clandestine, underground tunneling along the border in order to smuggle persons and goods into the United States is a serious and growing concern. Tunnel detection was a priority capability gap identified in our Border Security IPT as well, and needing a technical solution. However, there are currently no promising near-term technologies to detect underground tunnels efficiently that supports the Border Patrol's operations. The detection of smuggling in these tunnels requires a combination of both direct and indirect methods to determine the shape, size, position of the tunnel, geophysical characteristics, and understanding of the various detection methods.

The basic research area intends to study and characterize the geophysical characteristics of key border regions, examine the limitations of current detection methods, assist in advancing those detection methods, and examine the potential for new, complementary detection methods. This research and other new discovery is necessary so that future technology development of an effective tunnel detector will be possible. So, you can see how the basic research tunnel investment will directly support and be complementary to our transition and innovation R&D efforts.

Our innovation portfolio supports a key goal to put advanced capabilities into the hands of our customers as soon as possible as well. This is a high-risk research area, as compared to the low-risk product transition area, but if successful can be a game changer and provide new and improved operational capability to our component customers. An example is another tunnel detection effort. We are exploring additional, novel approaches to tunnel detection, including experimenting with UAV-mounted digital, electromagnetic, and gravity gradiometers, to determine their effectiveness and reliability. If successful, this will provide a wide-area search capability for rapid tunnel detection, potentially suitable to the Border Patrol. This demonstration may fail, but if successful will be a great game changer in our ability to protect the border.

Another innovative program includes DHS partnering with DOD and the ongoing global observer Joint Concept Technology Demonstrator, JCTD, which offers the potential for DHS to provide persistent, airborne, wide-area surveillance along our borders and coasts. In cooperation with CBP and the Coast Guard, S&T is plan-

ning a demonstration for employing maritime radar on an unmanned aircraft to detect and help prosecute drug-running boats off the Florida coast, for example—

Mr. MITCHELL. Could you wrap it up, Mr. Hooks?

Mr. HOOKS. Yes, sir. Sorry.

In summary, DHS is dedicated to being a customer-focused, output-oriented organization. Thank you.

Mr. MITCHELL. Thank you. Mr. Kapos.

[The prepared statement of Mr. Hooks follows:]

PREPARED STATEMENT OF ROBERT R. HOOKS

Good morning, Chairman Wu, Congressman Gingrey and distinguished Members of the Subcommittee. I am Robert Hooks, and I am the Director of the Transition Portfolio for the Science and Technology Directorate of the Department of Homeland Security, and I am pleased to appear before you today to discuss successes that the Department of Homeland Security's Science and Technology Directorate has achieved with respect to technology solutions on our borders.

As you are aware, Under Secretary Cohen is on travel and I am honored to appear before you in his place. Under Secretary Cohen asked me to express his appreciation and thanks to this committee, your staff, and the entire Congress, for the strong, bipartisan leadership and support you have given him and the men and women of the Science and Technology Directorate as we work to make the Nation safer.

Introduction to the DHS S&T Organization

Nearly 14 months ago, with Congress' support, Under Secretary Cohen implemented a new organizational structure for the Science and Technology Directorate to make it customer focused and output oriented. Our customers are the operating components and directorates of DHS, and their stakeholders are the State, local and tribal governments, first responders and private sector entities. Our Science and Technology effort to deliver technology is primarily organized into three portfolios: Basic Research, Innovation, and Product Transition.

Introduction to the Basic Research Portfolio

The 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, long-term research investment has the potential to lead to paradigm shifts in the Nation's homeland security capabilities.

In support of this objective for long-term research and development, we are in the process of establishing additional university-based Centers of Excellence in critical homeland security mission areas, including a Center for Excellence for Border Security and Immigration and a Center of Excellence for Maritime, Island, and Extreme/Remote Environment Security. These centers will provide fundamental research to support the DHS goals of strengthening border security, maritime security, and interior immigration enforcement. These centers will also establish education programs in homeland security relevant to their specific mission areas. This will provide learning opportunities to support the development of the next generation of homeland security leaders. We are currently in the selection phase and expect to announce the institutions for the new Centers of Excellence this month.

Tunnel Detection is an example of the type of focused, long-term research effort that we would tackle in the basic research area. As you are probably aware, the threats posed by clandestine underground tunneling along the border in order to smuggle persons and goods into the United States are a serious and growing concern. Detection of these smuggling tunnels requires a combination of both direct and indirect methods to determine the shape, size, and position of the tunnel, geophysical characteristics, and understanding of the various detection methods. If funded in fiscal year 2009, we intend to study and characterize the geophysical characteristics of key border regions, examine the limitations of current detection methods, assist in advancing those detection methods, and examine the potential for new complementary detection methods. The basic research tunnel investment will directly support and be complementary to our Transition and Innovation efforts.

Introduction to the Innovation Portfolio

The Innovation portfolio—Homeland Security Advanced Research Project Agency (HSARPA)—supports a key goal of Under Secretary Cohen's to put advanced capa-

bilities into the hands of our customers as soon as possible. Within the Innovation Portfolio, we have two overarching programs: High Impact Technology Solutions or HITS, and Homeland Innovative Prototypical Solutions or HIPS.

HITS are designed to provide proof-of-concept solutions within one to three years that could result in high-payoff technology breakthroughs. An example of a HITS is the tunnel detection effort. While we are in the process of awarding a contract as a result of a Broad Agency Announcement soliciting additional novel approaches to tunnel detection, we are also experimenting with UAV mounted digital electromagnetic gradiometers to determine effectiveness and reliability. If successful, this would provide a wide area search capability for rapid tunnel detection. This is high risk research, but if successful, can be a game-changer of new operational capability to our component customers and will complement our Transition and Innovation efforts.

HIPS are designed to deliver prototype-level demonstrations of game-changing technologies within two to five years. An example within the HIPS portfolio is the SAFECON project which is focused on developing an advanced screening capability at ports of entry. Sensors mounted on a crane interrogate shipping containers as the crane engages and lifts the container off of the ship. The sensors detect and identify dangerous cargo without impact to the normal flow of commerce. Our goal is to detect and identify dangerous cargo within 45 seconds or less.

Introduction to the Product Transition Portfolio

The Product Transition Portfolio, for which I am the Director, is centered on 11, functional, customer led, Capstone Integrated Product Teams (IPTs), three of which are Maritime Security, Cargo Security, and Border Security. In the Capstone IPTs, DHS operational components and directorates are the chairs or co-chairs and they define and prioritize capability gaps, then S&T offers technical solutions, and the customers are the final approval on if the offered technical solution is appropriate.

Specific to border security, our Border Security Capstone IPT is co-chaired by David Aguilar, Chief of the Border Patrol, and Luke McCormack, Chief Information Officer of Immigration and Customs Enforcement (ICE). For Cargo Security, Jayson Ahern, Former Assistant Commissioner for CBP's Office of Field Operations (OFO), was the original chair. His successor is Tom Winkowski, CBP's New Assistant Commissioner for Office of Field Operations. For Maritime Security, Rear Admiral Ron Hewitt, USCG, was the original chair. His successor is Rear Admiral Robert Parker, USCG, Assistant Commandant for Capability (CG–7).

While we have identified the principal stakeholders within the Capstone IPTs as chairs or co-chairs, they are not the only customer representatives to the IPTs. All DHS operational components and directorates are invited as customers to any Capstone IPT relevant to their mission. As an example, because of the inter-relationship within their respective geographic areas of responsibility, Coast Guard has representation on the Borders IPT, TSA, and DHS Policy office have representation on the Cargo IPT, and, CBP and ICE have representation on the Maritime Security IPT. Directed by the priorities of the Border, Cargo, and Maritime Security Capstone IPTs, we are developing technologies that can be delivered to the components in three years or less to assist in securing our maritime and land borders, and protect our Customs and Border Protection and Coast Guard law enforcement officers.

Introduction to the Borders and Maritime Security Division

The Borders and Maritime Security Division oversees the delivery of technologies to provide advanced detection, identification, apprehension and enforcement capabilities along land and maritime borders, and provide advanced technology spiral-development "injections" into the following program areas: Secure Border Initiative Network (SBI Net), Command 21, Secure Freight Initiative, Container Security Initiative, and Customs Trade Partnership Against Terrorism (C–TPAT).

Borders and Maritime Technologies Programs

A number of our programs focus on developing Detection, Classification, and Localization (DCL) sensor technologies to monitor illegal border activity with a wider range and greater accuracy than present-day technologies; command and control systems that deliver a much broader amount of information about current events to different levels of law enforcement; communications systems that provide connectivity to law enforcement officers working in remote locations; and modeling and simulation tools to help border enforcement agencies make informed improvements in immigration and border security policy and operations, as well as investments in technology, complex systems and infrastructure. These technologies and systems will help to ensure that maritime and border security assets are used efficiently and effectively and enable law enforcement to have access to robust and reliable intelligence when they need it.

Unmanned Aircraft for Border and Maritime Security Missions

We are continuing to actively develop technologies that will permit routine operation of UAVs for border and maritime security missions within the National Airspace System. In conjunction with the FAA and the DOD, we are developing an FAA-validated simulation that will be used, starting in FY09, to evaluate automated sense and avoid systems, the key enabler for safe and routine unmanned aircraft flight. DHS S&T is also partnering with DOD in the ongoing Global Observer Joint Concept and Technology Demonstration (JCTD), which offers the potential for DHS to provide persistent, airborne, wide area surveillance along our borders and coasts.

In cooperation with Customs and Border Protection and the Coast Guard, S&T is planning a demonstration for employing maritime radar on an unmanned aircraft to detect and help prosecute drug running boats off the Florida coast. We are actively pursuing, both outside DHS with the Departments of Commerce, Defense, and Transportation and inside DHS with CBP and the Coast Guard, the increased use of unmanned aircraft to secure our nation's borders and provide airborne capabilities for requirements that require extended station times.

Border Officer Tools Program

The officer tools and safety effort is developing and delivering technologies that will enable border security and Coast Guard members to perform their current tasks more efficiency, effectively, and with a higher level of safety. Development of these tools in many cases is leveraged from the initial investments of other government agencies, and then adapted to fit the operational environment and functions of several DHS security components. Where possible, technology is leveraged to support multiple DHS components. For example, the program will provide Coast Guard boarding officers with tools they carry onto vessels to perform inspections, which could be applied to CBP searches of over-the-road transportation. We are also developing tools that can be used by multiple DHS components to rapidly search vessels or vehicles, locate any hidden compartments, discriminate legitimate cargo from contraband, and remotely attain a positive identification of a person. We have recently developed and are not testing a pre-acquisition prototype of a repeater-based communications system that permits communication among boarding team members, no matter where they are in a ship. Repeaters are small transmission devices that are deployed like breadcrumbs as boarding officers enter and search a ship. The repeaters provide 100 percent connectivity between boarding team members in areas that previously allowed less than 50 percent connectivity without repeaters. In the future, we plan to make available a deployable communications repeater for boarding teams.

Cargo Security Efforts and Programs

Through our SAFECON (safe container) HIPS project, we are researching ways to quickly screen cargo at ports of entry. As a complement, we are also looking to improve supply chain security and thus decrease screening frequency and simultaneously increasing our probability of detection of dangerous contraband. Using a system-of-systems approach, we are developing advanced sensor and communication technologies within a security architecture that encompasses the world's supply chain. Some technologies developed in this program will enable CBP officers to identify tampering events and their location, track shipping containers, and ensure that alarm data is communicated reliably and securely. Most of these technologies will be commercialized, purchased by industry and adopted as an international standard that will meet DHS's core security requirements. Current project activities include the Advanced Container Security Device (ACSD), an in-container sensor to detect and warn of intrusion on any six sides, door openings or the presence of human cargo; Container Security Device (CSD), a small, low-cost sensor mounted within a container to detect and warn of the opening or removal of a container door; Marine Asset Tag Tracking System (MATTS), a remote and adaptive multi-modal global communications and tracking tag for transmitting security alert information from ISO shipping containers; Hybrid Composite Container, a potential next-generation, ISO approved, shipping container with embedded security sensors to detect intrusions that is more than 15 percent lighter than existing ISO steel containers and more durable; Advanced Screening and Targeting, a project that develops computer algorithms and software that will automatically collect, combine, analyze and find suspicious patterns in the shipping information of containers; and Supply Chain Security Architecture (SCSA), a framework for how near-term and future container-security technologies that will be incorporated by industry into supply chain security operations and how information can be communicated securely to CBP officer.

Technology Transition Process: Customer Focused and Output Oriented

As we develop these technologies, we recognize we need a disciplined process to ensure the technology is turned into widely distributed and utilized products and capabilities. Once the Capstone IPTs approve technical solutions, project level IPTs—S&T program managers working with component-customer program managers—are established to turn the proposed technical solutions into deliverable technology that is affordable and meets the customer's schedule and performance requirements. Through signed Technology Transition Agreements, S&T and our customers define and agree on schedule, performance requirements, transition paths, organizational responsibilities, integration strategy, technology transition readiness level, and estimated procurement, operating and support cost up front. This way, if initial procurement is too expensive, or operating costs are prohibitive, the decision to look for a new technology solution can be made early—before large buy acquisition programs are initiated and before federal, State, local, and tribal entities expend their precious resources.

Conclusion

In summary, DHS S&T is dedicated to being a customer focused, output oriented organization. Through the Capstone IPT process, our customers prioritize and decide on the incremental technology improvements most important to them. Informed by the Capstone IPTs, our basic research and innovation efforts provide the focused, protracted research and high impact advanced research for longer-term game changing technology solutions. We are dedicated to providing our customers—the DHS components and directorates, State, local and tribal governments, first responders and private sector entities—the technology necessary to succeed at their mission and protect our nation. That concludes my statement for the record. On behalf of Under Secretary Cohen, thank you for your support of the Science and Technology Directorate, and I welcome your questions. Thank you.

BIOGRAPHY FOR ROBERT R. HOOKS

Robert Hooks serves as the Director of Transition, in the Science and Technology Directorate of the Department of Homeland Security. In this role, Mr. Hooks is responsible for delivering near-term advanced technologies to the operational components of the Department to address their priority mission capability gap areas. Mr. Hooks communicates regularly with the component agencies of the Department to understand capability gaps and propose appropriate technology solutions that can transition into future component acquisition programs. Mr. Hooks then shares these desired technology solutions with other U.S. Government agencies, the private sector and International partners to identify the most appropriate providers. In addition, Mr. Hooks oversees the Department's SAFETY Act program which provides important legal liability protection to qualified Anti-Terrorism technologies, whether they are products or services.

Previously, Mr. Hooks served as the Chief of Staff for the Science and Technology Directorate and was responsible for the day-to-day management of the Directorate. He has also served as the Deputy Director in the Office of Research and Development where he oversaw the research, development, test and evaluation programs that were executed at the DHS federal laboratories, including the National Biological Analysis and Countermeasures Center, the Plum Island Animal Disease Center, the Transportation Security Lab, as well as within the Homeland Security elements of the DOE national laboratories. He oversaw the Homeland Security Stewardship Initiative, which included facilities construction and recapitalization, strategic partnerships with other government agencies, and Homeland Security focused workforce development and education programs that included a Scholars/Fellows Program and an integrated network of Homeland Security University Centers of Excellence.

Prior to joining the Department of Homeland Security in July 2003, Mr. Hooks served 20 years in the U.S. Navy in a variety of positions as a submarine officer, financial analyst, intelligence analyst, and personnel specialist. Mr. Hooks was the Contingency Budget Analyst in the Navy Budget Office where he was responsible for the Department of Navy's funding of military readiness and operations following the September 11th attacks and the wars against Afghanistan and Iraq. His sea tours were on both fast attack and ballistic missile submarines and included overseas deployments, special missions, and six Trident strategic deterrent patrols during the Cold War. He also served as an intelligence analyst for special programs at the National Security Agency where he authored several strategic intelligence assessments.

Mr. Hooks graduated from Cornell University with a Bachelor's of Science degree in Agricultural Engineering. He also holds a Master's of Administrative Science in

Financial Management from The Johns Hopkins University. He was selected to the Senior Executive Service in September 2005.

STATEMENT OF MR. ERVIN KAPOS, DIRECTOR, OPERATIONS ANALYSIS, SCIENCE AND TECHNOLOGY DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY; EXECUTIVE DIRECTOR, HOMELAND SECURITY SCIENCE AND TECHNOLOGY ADVISORY COMMITTEE (HSSTAC)

Mr. KAPOS. Good morning, Chairman Mitchell, Congressmen Gingrey and Hall, and other Members of the Committee. I am Ervin Kapos, Director of Operations Analysis for the Science and Technology Directorate of the Department of Homeland Security, and I am pleased to appear before you today to discuss my responsibilities concerning the oversight of the Homeland Security's Science and Technology Advisory Committee. And I must express my gratitude for somebody having introduced into the record its informal name, the HSSTAC, so I don't have to trip over its full name.

The HSSTAC was originally authorized in Section 311 of the Homeland Security Act for a period of three years, expiring on November 25, 2005. In October 2006, Section 302 of the *Safe Port Act,* and under Section 311 of the *Homeland Security Act,* reauthorizing the HSSTAC until December 31, 2008. The HSSTAC is chartered to be a source of independent scientific and technical planning advice for the Under Secretary for Science and Technology, with several objectives.

First, the committee advises the Under Secretary for S&T on organization of the Nation's scientific and technological resources, to prevent or mitigate the effects of catastrophic terrorism against the United States, and of catastrophic natural events. Second, it identifies research areas of potential importance to the security of the Nation, including matters relating to science, technology, research, engineering, new product development, including demonstration and deployment, business processes, emergency response, cargo security, technology, and other matters of special interest to the Department of Homeland Security.

Third, the HSSTAC assists the Under Secretary in establishing mission goals for the future. It advises on whether the policies, actions, management processes, and organizational constructs of the Science and Technology Directorate are focused on mission objectives. It advises on whether the research, development, test evaluation, and systems engineering activities are properly resourced to accomplish the objectives. It also identifies outreach activities and reviews the technical quality and relevance of the Directorate's programs.

Finally, upon request, the HSSTAC provides scientifically- and technically-based advice to the Homeland Security Advisory Council. Conversely, the committee draws, when needed, on the expertise of outside advisory groups for independent advice on specific technical and policy matters.

The HSSTAC has changed its modus operandi in the past year. It is now focused predominantly on certain high-priority issues that the Under Secretary has identified for it. At present, the HSSTAC is tasked with reviewing the threat that is expected from impro-

vised explosive devices, IEDs, in the United States in the next five and more years, and recommending Science and Technology investments to counter this threat in the future.

I believe, as does Mr. Cohen, that the HSSTAC provides the S&T Directorate valuable, independent, scientific and technical planning advice. We appreciate and support your efforts to extend the HSSTAC authority to 2012. Under Secretary Cohen appreciates your support of the S&T Directorate.

I shall welcome your questions. Thank you very much.

Mr. MITCHELL. Thank you. Dr. Jackson.

[The prepared statement of Mr. Kapos follows:]

PREPARED STATEMENT OF ERVIN KAPOS

Good morning, Chairman Wu, Congressman Gingrey and distinguished Members of the Subcommittee. I am Ervin Kapos, Director of the Operations and Analysis Division for the Science and Technology (S&T) Directorate of the Department of Homeland Security, and I am pleased to appear before you today to discuss my responsibilities concerning the oversight of the Homeland Security Science and Technology Advisory Committee (HSSTAC).

The HSSTAC was originally authorized in Section 311 of the *Homeland Security Act* (P.L. 107–296) for a period of three years, expiring on November 25, 2005. In October 2006, Section 302 of the *SAFE Port Act* (P.L. 109–347) amended section 311 of the *Homeland Security Act* reauthorizing the HSSTAC until December 31, 2008.

The HSSTAC is chartered to be a source of independent scientific and technical planning advice for the Under Secretary for S&T with several objectives. First, the Committee advises the Under Secretary for S&T on organizing the Nation's scientific and technological resources to prevent or mitigate the effects of catastrophic terrorism against the United States, and of catastrophic natural events.

Second, it identifies research areas of potential importance to the security of the Nation, including matters relating to science, technology, research, engineering, new product development (including demonstration and deployment), business processes, emergency response, cargo security technology, and other matters of special interest to the Department of Homeland Security.

Third, the HSSTAC assists the Under Secretary in establishing mission goals for the future. It advises on whether the policies, actions, management processes, and organization constructs of the Science and Technology Directorate are focused on mission objectives. It advises on whether the research, development, test, evaluation, and systems engineering activities are properly resourced to accomplish the objectives. It also identifies outreach activities and reviews the technical quality and relevance of the Directorate's programs.

Finally, upon request the HSSTAC provides scientifically- and technically-based advice to the Homeland Security Advisory Council. Conversely, the Committee draws, when needed, on the expertise of outside advisory groups for independent advice on specific technical and policy matters.

At present, the HSSTAC is tasked with reviewing the threat that is expected from Improvised Explosive Devices (IED) in the United States in the next five and more years, and recommending Science and Technology investments to counter this threat in the future. I believe, as does Mr. Cohen, that the HSSTAC provides the S&T Directorate valuable, independent scientific and technical planning advice. We appreciate and support your efforts to extend the HSSTAC Authority to 2012. Under Secretary Cohen appreciates your support of the S&T Directorate, and I welcome your questions. Thank you.

BIOGRAPHY FOR ERVIN KAPOS

Introduction

Mr. Kapos was born in Transylvania (Romania) in 1931, and lived in Cyprus from 1938 to 1950. He then came to the United States and attended Indiana University, studying mathematics at both the undergraduate and graduate levels for eight years, before moving to the Washington, D.C. area. He now lives in McLean, Virginia, with his wife June, a professional potter; their daughter Valerie, a tropical botanist, lives in Cambridge, England, with her husband and two daughters. Mr. Kapos was a Founding Director of MORS in 1966, Vice President and a member of

the Council on Military Operations Research Symposia, and was a Chartering Officer for MAS, the Military Applications Section (now a Society).

Education

Mr. Kapos completed a B.A. in Mathematics at Indiana University in 1954 and completed Ph.D. course work in Mathematics, also at Indiana University. At Indiana University, Mr. Kapos was a Teaching Associate in the Department of Mathematics and a Research Associate in the Institute of Educational Research.

Experience

Mr. Kapos joined the Navy's Operations Evaluation Group (OEG) (later an element of the Center for Naval Analysis) in 1958, immediately after leaving graduate school and remained there for almost 15 years. He served several tours as an analyst in the fleet, mainly with Pacific Fleet Commands, including OPTEVFORPAC, First Fleet, and CINCPACFLT. He also established and directed first-of-their-kind operations analysis programs in Command and Control and in Operational Intelligence. During the period from 1967 to 1972, he was successively Director of CNA's Southeast Asia Combat Analysis Division, Marine Corps Operations Analysis Group, and Operations Evaluation Group.

Mr. Kapos was senior OEG Representative on the staff of the Commander-in-Chief, Pacific Fleet, Commander, First Fleet, and the Commander, Operational Test and Evaluation Force. He conducted extensive analyses of combat operations in Southeast Asia, concentrating on the effectiveness of air and surface interdiction and on techniques of defense suppression. Other efforts involved test and exercise design, reconstruction and analysis in a variety of naval warfare and support areas, but with particularly heavy emphasis on communications, command and control. Mr. Kapos also developed a unique concept of intelligence analysis that culminated in a major Navy-supported study program know as "Red Side Operations Analysis."

Mr. Kapos was Director of the Marine Corps Operations Analysis Group, CNA. He managed the principal operational and systems analysis organization supporting the Commandant, U.S. Marine Corps and the Fleet Marine Forces. Earlier, Mr. Kapos was Director of the Southeast Asia Combat Analysis Division and directed analyses of the operations and effectiveness of Naval forces in Southeast Asia. Before that he was Leader of the Communications, Command and Control Team, where he pioneered the application of operations analysis in those areas.

Mr. Kapos was Director of the OEG for three years. He managed almost 100 civilians and military analysts. Programs included a field organization of 40 professionals at about 30 Navy operating commands, and a headquarters analysis effort totaling about 60 professionals that covered the range of Navy warfare and support disciplines.

Joining Ketron, Inc. in late 1972 as Vice President and Director of Washington Operations, Mr. Kapos became Executive Vice President in 1976 and President in 1980. He was personally involved in many of the naval warfare and support studies carried out in Ketron. He was most heavily engaged in analytical support to planning studies affecting naval surface warfare and command support, evolving concepts and objectives for tactical development and evaluation in the Navy, new concepts for readiness evaluation, the application of operations analysis to problems in operational intelligence, and the development of new approaches to the use of gaming and simulation for command and management training.

He was the founding principal and President of Kapos Associates Inc. (KAI) from 1984 to 2000. In KAI, Mr. Kapos evolved a complex, integrated program structure of policy studies, operational analysis and executive level gaming that, while initially focused on naval issues, also served clients up to Cabinet level, including various interagency bodies, executive departments, military services, and regional commands, as well as the private sector. In substantive content, the projects he pioneered and directed ran the gamut of interagency coordination, crisis response and consequence management; both counter- and anti-terrorism; modeling and simulation; maritime, land and aerospace warfare mission areas; special operations, weapons of mass destruction, military operations other than war; readiness assessment and reporting, command and control, operational logistics, manpower requirements, and war-gaming.

Mr. Kapos has been Director of the Operations Analysis Program in the Office of Naval Research (ONR) since 2001. The program is intended both to establish OA as a tool for management decision-making in ONR and thus an internal service function, and to provide solutions to problems in analytical methodology that obstruct the application of OA in such key areas as readiness assessment, command and control, force protection, and experimentation.

Other Professional Experience, Honors

He received the Secretary of the Navy's Meritorious Public Service Citation as well as numerous letters of commendation from the Naval Fleet and Force Commanders. Mr. Kapos has been an Associate Member of the Defense Science Board, serving on the Naval Surface Warfare Panel in 1974–76, and the Summer Study on Training and Training Technology in 1982. In 1987–1988, he was a member of the DSB Task Force on Computer Applications to Training and War-gaming. He has been a member of the National Academy of Science/National Research Council Panel on Response to Casualties involving Ship-Borne Cargoes. Mr. Kapos also served on the National Security Agency Advisory Board in 1979–1982. He served on the Panel on Science and Technology and Center for Strategic and International Studies (CSIS), and was a member of the Panel on Crisis Management at CSIS.

STATEMENT OF DR. BRIAN A. JACKSON, ASSOCIATE DIRECTOR, HOMELAND SECURITY RESEARCH PROGRAM, THE RAND CORPORATION

Dr. JACKSON. Thanks very much. Chairman and distinguished Members, I thank you for inviting me to participate in today's hearing.

I was asked to testify specifically about a recently-completed RAND research project that was supported by the Department of Homeland Security's Science and Technology Directorate that looked at how adversaries, terrorist groups in particular, can undermine the effectiveness of security technologies by altering their behavior. The way such groups have responded to defensive measures is similar to how others who seek to cross the border illegally can and have responded to security efforts, making the lessons that the terrorist groups can teach us very relevant to today's discussion about future border security technologies.

The core message of my testimony today is that we must explicitly consider the risks that adversaries' adaptive behavior poses to the performance of our border security technologies when we craft our research and development plans. If we don't do so, we risk spending resources on defenses that ultimately will not deliver the protection that we expect them to.

Looking across a variety of terrorist groups, we found that when challenged by security efforts, they responded with a set of four counterstrategies that limited the effects that the defenses had on the groups' operations. Specifically, they changed their operational practices in ways that made the defenses less effective. They used new technologies of their own to counter them. They moved to alter or to avoid the defensive measures, and they attacked the security technologies directly.

My written testimony and the research underlying it document numerous examples of counter technology strategies that these groups put in place, but what we found overall is that, for most defensive measures, the groups could find ways to degrade their protective value. In some cases, the groups paid a significant price to get around defensive measures. For example, to evade border controls and the security fence being put around the Israeli border, Palestinian groups had to develop specialized ladders that could let them get over without triggering the detection technologies on top, or had to build elaborate tunnel systems to get under it, as we have heard is a challenge at our border. In other cases, the price to evade defensive measures was relatively small. For example, the Irish Republican Army determined that under some circumstances

at least an expensive surveillance and facial recognition system could be defeated by having their operatives wear inexpensive baseball caps.

Given what we found, we identified three principles that should be considered as next-generation measures are designed and implemented. The first is that there needs to be extensive testing of the robustness of new security measures before they are introduced. Focused red-teaming efforts, challenging the technologies with teams of capable individuals to see if we can discover new ways to penetrate them, is one way to do that assessment. Such red-teaming is accepted practice in many technology development efforts, but our study further emphasized how important it is. The need to assess new technologies' weaknesses also suggests that small-scale demonstration projects may be particularly valuable steps to include in technology programs whenever possible before expanding to large-scale demonstrations or technology deployment, particularly given the extensive border security protection challenge that we face in this country.

A second principle is that we should preserve as much flexibility as we can in the technologies that we deploy. Systems that aren't locked into specific modes of operation preserve the ability of border security organizations to respond when adversaries change their behavior. Explicitly considering the value of this flexibility as we assess new technologies is important, since flexible technologies may cost more than systems that are locked into only one operational mode. If we don't consider the value of that flexibility, it may be inadvertently sacrificed to cut costs.

The final principle is that the Nation should maintain a diverse and flexible border security research, development, tests, and evaluation portfolio. If we devote all our resources to optimizing a single line of defense, there may be no backup available if that line is breached. Even if multiple defensive options are not all deployed, a portfolio approach to developing measures can provide fallback options if an initial defense becomes obsolete.

Depending on the level of the adaptive threat we face, the Nation might actually be better off having multiple defensive options of average effectiveness than concentrating on raising the performance of a single technology to the highest effectiveness possible, in terms of thinking about this as an overall system.

When faced with an adaptive challenge, the bottom line from our work is that we need to be prepared to adapt in return. The potential that adversaries might break through a defense soon after its introduction must be carefully assessed and included in our decision-making. Not doing so risks making large investments whose eventual benefits may not justify their costs. In designing protective measures, it shouldn't be immediately assumed that the newest and most advanced technologies give us the best protection. Sort of going to our title of our report, drawing on the common metaphor for defense efforts of building a fortress, relying on formidable but static defensive measures is a rather fragile and tenuous strategy, because once a wall is breached, there may not be anything left to protect you.

Depending on the adaptive capabilities of the adversary, a defensive model built on variety, where we have a number of security

measures that can be adjusted and redeployed as their vulnerable points are discovered, is a superior approach.

I would like to thank you again for the opportunity to address the committee, and look forward to your questions.

Mr. MITCHELL. Thank you. Chief Self.

[The prepared statement of Dr. Jackson follows:]

PREPARED STATEMENT OF BRIAN A. JACKSON[1]

Developing Robust Border Security Technologies to Protect Against Diverse and Adaptive Threats[2]

Chairman and distinguished Members: Thank you for inviting me to speak on the issue of border security technology as the House Science and Technology Committee begins the process of considering legislation focused on developing the next generation of border and maritime security technologies. I was asked to provide testimony about a recently completed RAND research effort for the U.S. Department of Homeland Security, Science and Technology Directorate, Office of Comparative Studies, focusing on the role of technology in homeland security activities.[3] As part of homeland security efforts, technology systems play a key role within a larger, integrated strategy to counter the efforts of violent and criminal organizations and to protect the public. Information and detection technologies gather data on individuals, vehicles, and behaviors; are used to monitor sites and areas of concern (including border information systems aimed at identifying individuals who should be not allowed to enter the country); help detect concealed weapons or contraband; and manage collected information so such information can be drawn on later to guide security decisions. Technologies such as barriers and setbacks harden targets or deny individuals access to the areas they want to enter or attack. Technologies such as communication systems coordinate response activities to increase the chances that terrorist or other illegal activities can be interdicted and stopped.

Our work has examined security technologies in the context of long-term conflicts between law enforcement and security organizations and terrorist groups. Much of this research focused on how the effectiveness of security technologies can degrade as our adversaries adapt and alter their behavior in response to the introduction of defensive measures.[4] That adaptive behavior can pose a significant risk to the security benefits new defensive technologies are intended to provide and, therefore, must be considered in technology planning. The testimony provided today is drawn

---

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of RAND or any of the sponsors of its research. This product is part of the RAND Corporation testimony series. The series records testimony presented by RAND associates to federal, State, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

[2] This testimony is available for free download at *http://www.rand.org/pubs/testimonies/294/*

[3] The results of this research effort have been published in a series of RAND reports focusing on the use of technology by terrorist groups and security organizations combating terrorism: *Breaching the Fortress Wall: Understanding Efforts to Overcome Defensive Technologies,* Brian A. Jackson et al., RAND MG–481–DHS, 2007, available at *http://www.rand.org/pubs/monographs/MG481/*; *Sharing the Dragon's Teeth: Terrorist Groups and the Exchange of New Technologies,* Kim Cragin et al., RAND MG–485–DHS, 2007, available at *http://www.rand.org/pubs/monographs/MG485/*; *Stealing the Sword: Limiting Terrorist Use of Advanced Conventional Weapons,* James Bonomo et al., RAND MG–510–DHS, 2007, available at *http://www.rand.org/pubs/monographs/MG510/*; *Network Technologies for Networked Terrorists: Assessing the Value of Information and Communication Technologies to Modern Terrorist Organizations,* Bruce W. Don et al., RAND TR–454–DHS, 2007, available at *http://www.rand.org/pubs/technical—reports/TR454/*; *Freedom and Information: Assessing Publicly Available Data Regarding U.S. Transportation Infrastructure Security,* Eric Landree, et al., RAND TR–360–DHS, 2007, available at *http://www.rand.org/pubs/technical_reports/TR360/*

[4] See *Breaching the Fortress Wall: Understanding Efforts to Overcome Defensive Technologies,* Brian A. Jackson, et al., RAND MG–481–DHS, 2007, available at *http://www.rand.org/pubs/monographs/MG481/*

from this research and focuses on the parts of the study that specifically address technologies relevant to border security.[5]

Although preventing a terrorist attack is one reason for the security measures at our nation's borders, it is not the only goal those measures are intended to achieve.[6] It is estimated that several hundred thousand individuals enter the United States illegally each year.[7] Most people seeking to cross the U.S. border illegally are not doing so to conduct terrorist activities. Rather, they are seeking to enter the country themselves, smuggle drugs, move other illicit goods, or engage in human trafficking. The shipping of illicit cargo through legitimate means—e.g., through the container shipping system—is also a concern. Although such individuals and groups are not motivated by the same factors as terrorist groups, they are nonetheless similarly determined to succeed and will respond to defensive measures placed in their path to hinder them. As a result, the broader lessons we identified about designing technologies that are robust to terrorist group adaptation are similarly relevant to the other challenges and threats that border protections are designed to address.

The core message of my testimony today is that in our technology planning and development we must explicitly consider the risk to the performance of our border security technologies that is posed by the competitive, action-reaction dynamic that exists between our security efforts and the adversaries they target; if we do not do so, we risk spending resources on defenses that ultimately will not deliver the protection we expect. To do so we must

- include testing, red-teaming, and experimentation in technology development efforts to ensure new security measures are robust to adversary adaptation
- maintain flexibility in our security technologies to the extent possible so we can respond to changes in the behavior of our adversaries that degrade or eliminate the protection the systems provide
- ensure *defense in depth* by developing portfolios of defensive measures that provide "fall back" options if adversaries learn how to avoid our primary defensive systems

Finally, although the focus of today's hearing is on developing technology, we must also remember that security is ensured not by technical systems alone but also by the organizations and people who use them and the concepts of operation that guide how they are used.[8] How we use technologies is a key determiner of how vulnerable or robust technologies are to our adversaries' adaptive efforts and helps to determine the net security effect of adversaries' efforts to break through our defenses. As a result, how technologies will be used in border security efforts should be considered during technology planning and research roadmapping to make sure we capture the full set of factors that will define their future security performance.

How Can The Responses of Terrorist Groups or Other Adversaries Affect the Protective Value of Security Technologies?

New security technologies are frequently costly, making it imperative that we ensure, to the extent possible, that they will produce enough benefits in improved security to justify the investments required to develop and deploy them. If there is a substantial risk that the security benefits of a particular technology will not be realized, that risk could make an otherwise promising technology a poor choice.

---

[5] While these remarks draw both on my work and that of my co-authors and colleagues, the specific content of my testimony is my responsibility alone. Additional information on RAND's research relevant to border security challenges is included in Michael A. Wermuth and K. Jack Riley, "The Strategic Challenge of Border Security," Testimony before the Committee on Homeland Security, Subcommittee on Border, Maritime and Global Counterterrorism, U.S. House of Representatives, March 8, 2007, available at *http://www.rand.org/pubs/testimonies/CT275/*

[6] U.S. Customs and Border Protection, Office of Border Patrol, "National Border Patrol Strategy," undated.

[7] See, for example, estimates in Government Accountability Office, "Illegal Immigration: Border-Crossing Deaths Have Doubled Since 1995; Border Patrol's Efforts to Prevent Deaths Have Not Been Fully Evaluated," GAO–06–770, August 2006.

[8] See, for example, David Aguilar, Office of Border Patrol, "Border Security: Infrastructure, Technology and the Human Element," Testimony Before the Subcommittee on Border, Maritime and Global Counterterrorism, Committee on Homeland Security, U.S. House of Representatives, February 13, 2007; RADM David P. Pekoske, U.S. Coast Guard, "Border Security: Infrastructure, Technology and the Human Element," Testimony Before the Subcommittee on Border, Maritime and Global Counterterrorism, Committee on Homeland Security, U.S. House of Representatives, February 13, 2007; and Jay Cohen and Gregory Giddens, Department of Homeland Security, "How Can Technologies Help Secure Our Borders?" Testimony Before the Committee on Science, U.S. House of Representatives, September 13, 2006.

In our research, we examined one such risk: How changes in behavior by terrorist groups could reduce or even eliminate the protective value of technological security measures. To identify how technologies were vulnerable to terrorist group adaptation, we looked at how a number of such organizations responded when they were challenged by new defensive measures. Because we were interested in lessons relevant to today's homeland security context, we examined four comparatively sophisticated terrorist groups that were in conflict with sophisticated states:

- Palestinian terrorist groups in Israel
- Jemaah Islamiyah (JI) and affiliated groups in Southeast Asia
- Liberation Tigers of Tamil Eelam (LTTE) in Sri Lanka
- Provisional Irish Republican Army (PIRA) in the United Kingdom

We found that the groups responded to security measures put in place by states or across regions with a set of four counter-technology strategies to limit the effect of the defenses on their operations. Specifically, they *changed their operational practices in ways that made the defenses less effective, used new technologies of their own to counter them, moved to avoid the defensive measures, and attacked the security technologies directly.* U.S. experience with individuals and organizations seeking to cross our border illegally shows these same broad strategies are relevant to help design current efforts to secure the country and to develop the technological tools needed to do so.

To illustrate the effect that groups changing their behavior has on the effectiveness of defensive measures, I discuss here a few of the ways the terrorist groups we studied reduced the effectiveness of protective technologies, circumvented the technologies entirely, and even attacked or corrupted the defensive measures that were getting in their way.

In many cases, terrorist groups found ways to change their behavior to render protective measures less effective. For example, the majority of the four terrorist groups responded to weapons-detection technologies by breaking down their weapons materials into small quantities (such as smuggling explosives in toothpaste tubes or cookie tins) or otherwise shielding them from detection technologies to enable smuggling or attack operations. The various ways they did this included shipping explosives obscured by strong-smelling spices or hiding them in noxious cargoes like rotting fish to conceal their odor from dogs or confuse other detectors.

PIRA spent considerable time conducting "challenge-response" studies to determine the limitations of surveillance systems in an effort to learn what the systems could and could not detect and to assess the areas they covered. The group then used that knowledge to operate in ways and at times that were less likely to be detected. For example, armed with the knowledge that specific weather and lighting conditions made some sensors less effective, PIRA planned its movements and operations accordingly.

The strategies we discovered in our case studies are similarly relevant to the Nation's border security challenges. For example, in 2004 testimony before the House Select Committee on Homeland Security, Lawrence Wein of Stanford University raised questions about whether terrorist groups could render the fingerprint biometric scanning done by the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program less effective by selecting operatives whose fingerprints either will not scan well or have been deliberately altered to defeat the scanning.[9] It is also well known that smugglers seeking to bring illegal narcotics and other materiel into the country frequently alter their operational practices to conceal their cargoes from search-and-detection approaches.

When they could do so, terrorist groups avoided defensive measures entirely, neutralizing their protective benefits. To avoid identification requirements and databases used to flag known or suspected operatives, most groups relied on false documents and identification credentials to hide the true history and identity of both people and vehicles. Some groups even took this strategy to the extreme, coercing innocent people with no connection to terrorism—by threatening their lives or the lives of their loved ones—to transport people or weapons through checkpoints with identity checks.

Avoidance can work for surveillance systems as well: As part of Israeli security measures, overhead surveillance with unmanned aerial vehicles (UAVs) or helicopters were used to monitor areas near the border where attacks were staged. In rural areas, Palestinian groups used spotters on rooftops in the West Bank or Gaza

[9] Lawrence M. Wein, "Disrupting Terrorist Travel: Safeguarding America's Borders Through Information Sharing," Testimony before the U.S. House of Representatives, Select Committee on Homeland Security, September 30, 2004.

Strip to watch for the vehicles and warn militants to stay out of sight when the surveillance systems were in the area.

To avoid some defenses, groups had to make more drastic changes. In response to significantly strengthened border security at ports of entry in the nations where it operated, JI shifted its operations from seeking to move people and material through defended areas like airports to less monitored and defended maritime or land borders. In response to the security barrier erected around Israel, Palestinian groups reportedly deployed specially crafted ladders that enabled them to climb over the security fences without triggering the sensors at the top. In addition, the groups have also engaged in extensive tunneling to circumvent the barrier around Israel and border security between Egypt and Gaza, enabling weapons smuggling and infiltration. The Israeli Defense Force (IDF) notes that Palestinians have taken a number of measures to avoid having their tunneling operations detected, including building tunnels in residential areas (entrances are often through private homes and property), digging at night, transporting displaced dirt and sand out of the vicinity of the tunnels, and staging diversionary strikes against IDF outposts to conceal the sound of explosives.

At our own border, individuals seeking to enter the United States illegally have responded to the deployment of border fencing in similar ways, for example by altering their routes and seeking to enter the country at more remote, unfenced locations. Drug smugglers have similarly shifted their routes and transport modes to avoid interdiction efforts.[10] Tunneling under the barriers has also been observed.[11]

Finally, in some limited cases, terrorist groups simply attacked the defensive measures hindering their activities. In response to the extensive use of information systems in the counterterrorism effort against PIRA, the group sought to attack information systems directly to corrupt or steal information (at one point breaking into a police facility to steal files). The group also used information-gathering technologies such as the security organizations' own public tip line to inject false information into the system. The group also used hoax operations and triggered detection technologies to cause false alarms as ways to stress the capabilities of the security and response forces. In some cases, the groups we studied directly broke down barriers and defenses that got in their way, either by using larger bombs or by staging more complex operations to neutralize the defense before a larger attack took place. In response to the construction of fencing on the U.S. land border, similar efforts to damage or breach the barrier have been observed.[12]

How important were terrorist efforts to "learn their way around" defensive measures? For most defensive measures, the groups could find ways to reduce their effectiveness and degrade their protective value. However, in some cases, terrorist groups paid a substantial price to neutralize a defense; for example, although a tunnel might make it possible to get under a security barrier, the effort the group had to spend to construct it was effort that could not be devoted to violent activities. When this was the case, even if the technology did not necessarily deliver the full protection it was expected to—or deliver it in the way that was expected when it was designed—its value could still be considerable.

Then again, in other cases, the cost to the group to evade a defensive measure was relatively small; in one particularly dramatic case cited by a counterterrorism professional we interviewed, PIRA learned that a sophisticated surveillance system incorporating facial recognition technology could, under the right circumstances, be countered by simply wearing a baseball cap. In this case, it took the group very little effort to counter the technology.

Principles for Designing Defensive Technology Efforts

Given the costs of designing and implementing novel border security technologies, it is important to consider the threat that adversary adaptation poses to their eventual effectiveness and value during research, development, test, and evaluation planning, and implementation.[13] Looking across the terrorist groups we studied, we identified a number of principles that should be considered as next-generation measures are designed and implemented. In some cases, what our review of historical

---

[10] See, for example, discussion in Office of National Drug Control Policy, "Measuring the Deterrent Effect of Enforcement Operations on Drug Smuggling, 1991–1999," August 2001.

[11] See, for example, discussion in Blas Nuñez-Neto and Stephen Viña, "Border Security: Barriers Along the U.S. International Border," Congressional Research Service, RL33659, September 21, 2006.

[12] See, for example, discussion in Nuñez-Neto and Viña, 2006.

[13] Michael A. Wermuth and K. Jack Riley, "The Strategic Challenge of Border Security," Testimony Before the Committee on Homeland Security, Subcommittee on Border, Maritime and Global Counterterrorism, U.S. House of Representatives, March 8, 2007, available at *http://www.rand.org/pubs/testimonies/CT275/*

terrorist group behavior had to teach us was "not news": Some of the lessons merely reinforced the importance of principles already considered good practice in technology design and testing. However, in other cases, what they had to teach was less obvious. In all cases, the potential result of not learning the lessons is high: losing the opportunity to prevent terrorist attacks.

The Importance of Testing and "Red Teaming" Technologies

Terrorist groups' counter-technology efforts underscore the importance of extensively testing new security measures before they are introduced. To make sure new technologies will perform over time, designers need to assess what information adversaries would need to circumvent the technologies and identify how they might get access to that information. Can groups "test" a defense's capabilities by challenging it in different ways? If a measure's performance relies on keeping some details of its capabilities secret, how long can those secrets be kept? Furthermore, dedicated "red teaming" of new technologies—challenging them with teams of capable individuals to see if they can discover new ways to penetrate the security measures—is also critical. Such testing is established practice for many security technologies and measures. For example, when it comes to cyber security, companies routinely use "hackers" to challenge security measures the companies have put in place. The need to test new technologies and explore their possible weaknesses also suggests that small-scale technology demonstration projects and evaluation studies of promising technologies may be particularly valuable intermediate steps to include in technology programs whenever possible before they are expanded to larger-scale demonstration or technology-deployment efforts.

Maintaining Flexibility in Technology Design

Given that adversaries will almost certainly find ways to degrade the performance of even the best security technologies, we should preserve as much flexibility as possible in the technologies we design and deploy. If the design of a defensive measure locks it in to a single configuration or operating mode, its benefits are vulnerable to changes in adversary behavior. If the security measure is static[14], it will not be able to adjust to a dynamic threat. In contrast, if flexibility is built into the defense from the start—e.g., if, when a terrorist group "breaks the code" on how the defense functions, we can change the code and reconstitute performance—then the benefits provided by the defensive measure can be preserved. Just as the terrorists we studied were able to change their operational practices to get around defensive technologies—e.g., obscuring the signatures they were designed to detect, using deception, adjusting the speed or character of their operations—changes in operational practices could similarly provide a variety of strategies for altering the character of defensive systems. For example, maintaining the ability to redeploy surveillance systems or change how security forces respond to alarms from detection systems are ways that technological performance could be altered to respond to changes by adversaries.

Systems that are flexible—that are not locked into specific modes of operation—preserve the opportunity for border security organizations to adapt their performance to respond to changes made by individuals and organizations seeking to enter the country illegally. Considering the value of this flexibility in the evaluation of potentially new technologies is important, since providing such flexibility may require additional expenditures up front when the defense is designed and implemented. If it is not considered, options that could provide robustness may be inadvertently sacrificed in an effort to reduce costs.

Developing Portfolios of Defensive Options for Defense in Depth

The risk that adversaries will identify strategies to defeat or evade individual security measures also suggests that the United States should maintain a diverse and flexible border security research, development, test, and evaluation portfolio. If we devote all our resources to optimizing a single line of defense, there will be no backup available if that line is breached. This is one reason behind the idea of defense in depth—maintaining multiple lines of protection against high-risk threats.

Security planners should consider a variety of defensive technology options, maintaining possibilities for alternative approaches if currently effective technologies are neutralized. Even if multiple defensive lines are not all deployed at the same time,

[14] Depending on the security measure, the technological characteristics—e.g., the nature of a detection technology—could make it difficult or impossible to change in response to adaptation by an adversary. In other situations, the combination of technology and the way it is used—e.g., including the concept of operations, etc.—could make it possible to respond to countermeasures.

a portfolio approach to developing defensive measures could provide "fall back" options if an initial defense becomes obsolete. Depending on the level of adaptive threat, the Nation could be better off having multiple defensive options of average effectiveness than a single highly effective option without a viable back-up. If decisions are made to pursue a specific path, the costs of maintaining other technologies in reserve—perhaps not fully developed, but at a stage at which they might be called on if needed—should be considered as well. Such an approach is analogous to maintaining a diversified portfolio of investments, containing a variety of options, where comparatively small investments provide various hedges against different shifts in circumstances. Small-scale technology demonstration projects and evaluation programs can also help to pursue this strategy, since they can provide a cost-effective way to explore multiple security options and assess their relative performance and robustness.

Conclusions

When adversaries are successful in countering all or part of a defensive technology, the utility of the system may be significantly reduced or lost entirely. Such losses devalue the costs society pays to design, produce, field, use, and maintain the technology—where costs include not just financial and materiel costs but also less tangible costs such as reductions in privacy or the inconveniencing of individuals legitimately crossing U.S. borders, when such security measures are implemented. Given the scale of U.S. borders and the volume of individuals and goods that cross them everyday, those costs can be considerable.

As a result, "adaptive destruction" is one more risk that must be managed by the science and technology programs charged with developing novel border security capabilities. The potential that adversaries might break through a defense soon after its introduction must be assessed and included in the cost-benefit analyses that provide the basis for going forward with large-scale technology testing and procurement. Not doing so may lead to major investments whose eventual benefits may not justify their costs. The robustness of new defensive technologies against adversary adaptation must be explicitly considered in crafting a technology roadmap for next-generation border security technologies and in efforts to deploy current technologies on the borders.

Furthermore, although the focus of the discussion here is on technology, we must recognize how the technology choices we make affect the rest of the border security system and the how the interactions among the parts of that system shape the value of new technologies and defenses. Although an adversary's efforts to break through our defenses may be aimed at the technologies we use to protect ourselves, the impact of those efforts will be shaped by the concepts of operation around those technologies and the people charged with implementing them.

For example, if a new detection technology produces many false alarms (magnified perhaps by individuals or smuggling organizations intentionally triggering the sensors to undermine the value of the system) can such false alarms be dealt with quickly or will responding to them consume human resources that could be put to better use in other ways? If migrants and smugglers respond to border fencing and surveillance by regularly damaging the fence and its associated systems, how will a constant stream of repair efforts affect DHS's security efforts? If the defenses we deploy simply result in displacement (e.g., individuals shift from crossing the border at one location to another) are we better off, worse off, or the same from a security perspective?[15]

The answers to these questions depend not just on technology but on how all the elements of the border system work together, and their answers will partly determine how much of a threat adversaries' counter-technology efforts pose to the country.

Although technologies can provide an edge in protecting our borders, that edge can be dulled by adversaries' counter-technology efforts. An understanding of the way adversaries have responded to counter defensive technologies in the past underscores the complexity of designing new systems to protect society from the threat such adversaries pose. Our research suggests that, in designing protective measures, we should not immediately assume that the newest and most advanced technologies—the highest wall, the most sensitive surveillance—will provide the best

[15] For example, diversion of illegal entry traffic from urban to rural areas has been characterized as beneficial from a security perspective, because individuals crossing the border in an urban area can vanish quickly into traffic, thus considerably reducing the time for apprehension. (David Aguilar, "Border Security: Infrastructure, Technology and the Human Element," Testimony Before the Subcommittee on Border, Maritime and Global Counterterrorism, Committee on Homeland Security, U.S. House of Representatives, February 13, 2007.)

protection. Drawing on common metaphors for defensive efforts, a fortress—relying on formidable but static defensive measures—is a limiting strategy. Once a wall is breached, the Nation is open to attack. Depending on the adaptive capabilities of the adversary, a defensive model built from a variety of security measures that can be adjusted and redeployed as their vulnerable points are discovered provides a superior approach. However, whatever combination of models and measures is chosen, it is only by exploring adversaries' potential counter-technology behaviors that vulnerabilities in current and potential future defensive measures can be discovered and addressed.

I would like to thank you again for the opportunity to address the committee today on this important topic, and I look forward to answering any questions you might have.

BIOGRAPHY FOR BRIAN A. JACKSON

Brian A. Jackson is Associate Director of the Homeland Security research program at the RAND Corporation. His terrorism research has focused on tactical and operational learning by terrorist groups and terrorist groups' use of technology. Individual projects have developed approaches to assess the threat posed by potential terrorist use of specific weapons, examined of the strategies to respond to terrorist targeting of national economies, constructed terrorist attack scenarios to support policy analysis efforts, and examined emergency response strategies and incident management for responses to major disasters and terrorist attacks. Key publications in these areas include articles in *Studies in Conflict and Terrorism* and *Military Review* on technology adoption by terrorist organizations, terrorist organizational structures and behavior, and intelligence gathering for targeting terrorist and insurgent groups, as well as the RAND reports *Aptitude for Destruction, Volumes 1 & 2,* examining organizational learning in terrorist groups, *Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies,* and Volumes 1 and 3 of the RAND *Protecting Emergency Responders* series of publications. Brian holds a Ph.D. in bio-inorganic chemistry from the California Institute of Technology and a Master's degree from George Washington University in Science, Technology, and Public Policy.

STATEMENT OF CHIEF JEFF SELF, DIVISION CHIEF, U.S. BORDER PATROL

Mr. SELF. Thank you, Chairman Gordon, for your opening remarks, Congressman Mitchell, Ranking Members Hall and Gingrey, and other distinguished Subcommittee Members.

It is my honor to appear before you today to discuss the Office of Border Patrol's use of technology in securing the border. My name is Jeff Self. I am the Division Chief responsible for Southwest border operations for Customs and Border Protection's Office of Border Patrol.

The United State's Border Patrol is a component of the Department of Homeland Security, DHS, U.S. Customs and Border Protection. I would like to begin by giving you a brief overview of agency and mission. Since 1924, the Border Patrol has grown from a handful of mounted agents patrolling desolate areas along the U.S. border to today's highly trained, dynamic workforce of almost 15,000 men and women supported by sophisticated technologies, vehicles, aircraft, and other equipment.

Contributing to all this is the Border Patrol's time-honored duty of interdicting those who illegally enter the United States or smuggle narcotics and contraband between ports of entry. The Border Patrol's national strategy is an all threat strategy with anti-terrorism as our main priority. We cannot protect against the entry of terrorists and the instruments of terror without also reducing the clutter that is caused by illegal migration across our borders. This strategy has increased the effectiveness of our agents by using

a risk management approach to deploy our resources. This strategy recognizes that we cannot go it alone. Border awareness and cooperation with our law enforcement partners are critical to securing America's borders.

We cannot control our borders by merely enforcing law at the line. Our strategy incorporates defense-in-depth components, including transportation checks away from the physical border. To carry out its mission, the Border Patrol has a clear strategic goal to establish and maintain effective control of the borders of the United States. Effective control is defined in the Border Patrol strategy as ability to detect, respond, and interdict border penetrations in the areas deemed a high priority for threat potential or other national security objectives.

In order to establish effective control in a given geographical area, we must be able to consistently detect an illegal entry, identify and classify the entry, and determine the level of threat involved, respond to the entry, and bring the event to a satisfactory law enforcement resolution. Gaining, maintaining, and expanding a strong enforcement posture with sufficient flexibility to address potential exigent enforcement challenges is critical in bringing effective control to the borders. Guidance at the national level for planning and implementation ensures resources are initially targeted to gain and maintain effective control in the most vulnerable, high risk border areas, and then to expand this level of border control to all Border Patrol sectors.

While the key is the right combination of personnel, infrastructure, and technology, it must be coupled with improved rapid response capability and organizational mobility. Each of these components is interdependent, and is critical to the success of the Border Patrol strategy. There is no stretch of the border in the United States that can be considered completely inaccessible or lacking in the potential to provide an entry point for a terrorist or terrorist weapon.

Therefore, securing every mile of diverse terrain is an important and complex task that cannot be resolved by a single solution. To secure each unique mile of the border requires a balance of technology, infrastructure, and personnel that maximizes the government's return on investment, and is tailored to each specific environment.

The Border Patrol operates in three basic geographical environments: urban, rural, and remote. Each of these environments requires a different mix of resources. In an urban environment, enforcement personnel generally have only minutes or sometimes seconds to identify an illegal entry and bring the situation to a successful law enforcement resolution. In rural and remote areas, where enforcement personnel have minutes to hours, or hours to days to detect, identify, classify, respond, and resolve, we expect to incorporate a comprehensive technological solution.

Continued testing, acquisition, and deployment of sensing and monitoring platforms will be crucial in addressing these vast areas along America's borders. Nationally, the Border Patrol is tasked with a very complex, sensitive, and difficult job, which historically has presented immense challenges. We face those challenges every day with vigilance, dedication to service, and integrity, as we work

to strengthen the national security and protect America and its citizens.

I would like to thank both Chairman Wu and the subcommittee for the opportunity to present this testimony today, and for your support of CBP and DHS.

I look forward to answering any questions that you may have.

[The prepared statement of Chief Self follows:]

PREPARED STATEMENT OF JEFF SELF

Chairman Wu, Ranking Member Gingrey, and distinguished Subcommittee Members, it is my honor to appear before you today to discuss the Office of Border Patrol's use of technology in securing the border. My name is Jeff Self, and I am the Division Chief over Southwest Border for Customs and Border Protection's Office of Border Patrol. The United States Border Patrol is a component of the Department of Homeland Security's (DHS) U.S. Customs and Border Protection (CBP). I would like to begin by giving you a brief overview of our agency and mission. As the guardian of the Nation's borders, CBP safeguards the homeland—foremost, by protecting the American public against terrorists and the instruments of terror, while at the same time enforcing the laws of the United States and fostering the Nation's economic security through lawful travel and trade. Since 1924, the Border Patrol has grown from a handful of mounted agents patrolling desolate areas along U.S. borders to today's highly-trained, dynamic work force of almost 15,000 men and women supported by sophisticated technology, vehicles, aircraft, and other equipment. Contributing to all this is the Border Patrol's time-honored duty of interdicting illegal aliens and narcotics and those who attempt to smuggle them across our borders. We cannot protect against the entry of terrorists and the instruments of terror without also reducing the clutter that is caused by illegal migration across our borders. For example, today we have to account for all who enter or attempt to enter the United States illegally. Last year we arrested over 870, 000 people who entered the United States illegally. Of those, we had over 18,000 major crime hits through biometric technology. These crime hits canvassed a litany of crimes to include murder, rape, sexual assaults, and kidnapping. It is imperative that we reduce the number of persons or clutter attempting to illegally enter the United States so that we can concentrate on terrorist or weapons of terror from entering the United States.

The Border Patrol's national strategy is an "all threats" strategy with anti-terrorism as our main priority. This strategy has made the centralized chain of command a priority and has increased the effectiveness of our agents by using a risk-management approach to deploy our resources. The strategy recognizes that border awareness and cooperation with our law enforcement partners are critical. Partnerships with the Department of the Interior; Immigration and Customs Enforcement; Drug Enforcement Administration; Federal Bureau of Investigation; State, local, and tribal law enforcement agencies; and State Homeland Security offices plays a vital role in sharing and disseminating information and tactical intelligence that assists our ability to rapidly respond to an identified threat or intrusion, which is essential to mission success.

Recognizing that we cannot control our borders by merely enforcing the law at the "line," our strategy incorporates a "defense in depth" component, to include transportation checks away from the physical border. Traffic checkpoints are critical to our enforcement efforts because they deny major routes of egress from the borders to smugglers who are intent on delivering people, drugs, and other contraband into the interior of the United States. Permanent traffic checkpoints allow the Border Patrol to establish an important second layer of defense and help deter illegal entries through comprehensive enforcement. Border Patrol Agents often encounter fraudulent documents while conducting transportation check duties. Agents receive training at the Border Patrol Academy that enables the agent to identify key features and characteristics of valid immigration documents. This training, coupled with on the job training, allows agents to identify common tactics used by the criminal element in creating fraudulent documents. Our most valuable asset at the checkpoint in examining the validity of any document (birth certificate, driver's licenses, and immigration documents) is the agent's experience.

To carry out its mission, the Border Patrol has a clear strategic goal: Establish and maintain effective control of the border of the United States. Effective control is defined in the Border Patrol's strategy as the ability to detect, respond, and interdict border penetrations in areas deemed a high priority for threat potential or other

national security objectives. In order to establish effective control in a given geographical area, we must be able to consistently:

- Detect an illegal entry;
- Identify/Classify the entry and determine the level of threat involved;
- Respond to the entry; and
- Bring the event to a satisfactory law enforcement resolution.

Gaining, maintaining, and expanding a strong enforcement posture with sufficient flexibility to address potential exigent enforcement challenges is critical in bringing effective control to the borders. Guidance at the national level for planning and implementation ensures resources are initially targeted to gain and maintain effective control in the most vulnerable, highest-risk border areas, and then to expand this level of border control to all Border Patrol Sectors.

While the key to mission success is the right combination of personnel, infrastructure, and technology, it must be coupled with improved rapid response capability and organizational mobility. Each of these components is inter-dependent and critical to the success of the Border Patrol's strategy. We are fully engaged with the DHS Science and Technology (S&T) Directorate in our efforts to identify, develop, and acquire technology to help us gain enhanced awareness and control of our borders. Our participation in S&T's Integrated Process Team on Border Security, for example, will help us use S&T resources to develop technology that will better secure our borders. Systems with the technological ability to predict, detect, and identify illegal entries and other criminal activity, but lacking the capacity for a rapid response or reaction, cannot complete the enforcement mission. Conversely, enforcement personnel with inadequate intelligence or poor technological support to provide situational awareness, access, and adequate transportation or equipment necessary to conduct enforcement activity are much less likely to be effective in today's dynamic border environment.

There is no stretch of border in the United States that can be considered completely inaccessible or lacking in the potential to provide an entry point for a terrorist or terrorist weapon. Therefore, securing every mile of diverse terrain is an important and complex task that cannot be resolved by a single solution, such as installing fence. Securing each unique mile of the border requires a balance of technology, infrastructure, and personnel that maximizes the government's return on investment and is tailored to each specific environment. Some of the components utilized in evaluating tactical infrastructure needs are border access (the existence of all-weather roads), border barriers (vehicle and pedestrian), and the lack of non-intrusive inspections equipment at checkpoint facilities.

The proper mix of personnel, technology, and infrastructure will vary with differing border environments and enforcement challenges. The Border Patrol operates in three basic geographical environments: urban, rural, and remote. Each of these environments requires a different mix of resources. In an urban environment, enforcement personnel generally have only minutes, or sometimes seconds, to identify an illegal entry and bring the situation to resolution. This dynamic is a result of the fact that significant infrastructure exists to facilitate an illegal entrant's approach to the border and entry and to permit the violator to escape within moments of effecting the entry by blending in with the legitimate traffic in the community. New tactics are constantly developed by those attempting to avoid detection in such situations in order to combat increased border security. One of those new methods that we have seen is the discovery of tunnels. There have been over 70 tunnels detected on the border. These tunnels were detected by various methods including sinking vehicles, collapsing roads, and by agents in the performance of their duties.

On the Northern border, the vastness and remoteness of the area and the unique socioeconomic ties between the U.S. and Canada are significant factors in implementing the Border Patrol's national strategy. Severe weather conditions on the Northern border during winter intensify the need to expand "force-multiplying" technology to meet our enforcement needs. The number of actual illegal border penetrations along the U.S.-Canada border is small in comparison to the daily arrests along the U.S.-Mexico border. The threat along the Northern border results from the fact that over ninety percent of Canada's population of 30 million lives within one hundred miles of the U.S.-Canada border. It is most likely that potential threats to U.S. security posed by individuals or organizations present in Canada would also be located near the border. While manpower on the U.S.-Canada border has significantly increased since 9/11, the Border Patrol's ability to detect, respond to, and interdict illegal cross-border penetrations there remains limited. Continued testing, acquisition, and deployment of sensing and monitoring platforms will be crucial in addressing the Northern border threat situation.

One tool that CBP uses to assist with border security is the Unmanned Aircraft System (UAS). The UAS provides CBP with a remotely piloted asset that allows for persistent, broad area surveillance. UAS operations are proactive responses to uncued, cued, and intelligence based missions. The UAS Program focuses its capabilities on the CBP priority mission and enhances surveillance and reconnaissance requirements along the border. The UAS has the flexibility and endurance to fly long leg surveillance missions while conducting both scheduled and unscheduled searches. As a law enforcement force multiplier for CBP, the UAS allows CBP Air and Marine (A&M) to support other DHS entities, including the United States Coast Guard, the Federal Emergency Management Agency (FEMA), and U.S. Immigration and Customs Enforcement.

Since 2004, CBP UASs have flown more than 2,000 hours, directly contributing to more than 4,000 arrests and the seizure of thousands of pounds of marijuana. In July 2007, CBP A&M added another UAS to the southwest border for a total of two. In FY 2008, one UAS will migrate to the northern border to support expanded northern border operations. Once additional personnel are trained to support UAS operations in the southwest, CBP A&M will be available to provide surveillance at the southwest border 24 hours a day, seven days a week.

Nationally, the Border Patrol is tasked with a very complex, sensitive, and difficult job, which historically has presented immense challenges. We face those challenges every day with vigilance, dedication to service, and integrity as we work to strengthen national security and protect America and its citizens. I would like to thank both Chairman Wu, and the Subcommittee, for the opportunity to present this testimony today and for your support of CBP and DHS.

DISCUSSION

Mr. MITCHELL. Thank you. At this point, we will open up for our first round of questions, and I will recognize myself for five minutes.

Dr. Jackson, you specifically mentioned how adversaries have been able to detect the technologies identified as priorities in the bill: unmanned surveillance vehicles, tunnel detectors, anti-counterfeit technologies, and so on. How should these identified vulnerabilities affect how DHS proceeds in these research areas?

Dr. JACKSON. Well, any technology is vulnerable. It is a question of how easy or how hard it is for those vulnerabilities to be discovered by our adversaries, and how quickly they can exploit them.

In thinking about—sort of dealing with that in research and development planning, one of the elements is to pursue different strategies simultaneously, so if they determine a way around a first line anti-counterfeiting technology, for example, there are ways that it can be modified to address that vulnerability.

But the other piece of this, too, it is something that I included in my written testimony, but not my oral, is that the other piece of this is the technology's function within the overall system of our border defense, and so, there is also the human resources and the concepts of operation better used to reinforce the effectiveness of those technologies.

And those can actually provide a way, by preserving flexibility in the way that we use the technologies, to preserve our ability to adapt in response as well. So it is sort of the two-pronged strategy of making sure that we have preserved variety in our technologies, but also, thought through how the way that we use those technologies can also counteract the adaptability of the folks who are trying to break through the border.

Mr. MITCHELL. Thank you. Chief Self, one of the things I would like to ask you—. First, how would you characterize DHS S&T's

interaction with the CBP, and has DHS S&T been responsive to the CBP's short and long-term technology needs?

Mr. SELF. I would characterize it, sir, as a very close relationship. Within the Office of Border Patrol, we have an Enforcement and Information Technologies Division with the Division Chief responsible for the personnel. They work closely with CBP Office of Information Technology, and together, coordinate with S&T.

There has been coordination on many efforts in research and development for operational technologies over the last couple of years.

Mr. MITCHELL. In your testimony, you say that our most valuable asset at the checkpoint in examining the validity of any document is the agent's experience. Does CBP currently employ anti-counterfeiting technology to help agents catch fraudulent documents? And if not, why, and in your opinion, what value does technology add to anti-counterfeit efforts?

Mr. SELF. As it now stands, sir, agents in the field basically rely on their training that they receive at the Academy. They receive 21 hours of training in fraudulent document identification. In addition, they are trained in how to look at the security features that are within the document, and after leaving the Academy, they have post-Academy, in which they receive additional training on fraudulent documents.

Other than that, there—at the present time, there is no technology for them to utilize in running cards through to identify that they have been altered or they are a false card.

Mr. MITCHELL. You rely strictly on the agent's experience, and what they learned?

Mr. SELF. That is correct, sir.

Mr. MITCHELL. All right. You mentioned that the Border Patrol operates in three distinct environments: urban, rural, and remote. Yet, research priorities are weighed towards technologies intended to operate in remote environments. What type of technology gaps exist for CBP operations in urban and rural environments, and why have these technologies not been a priority?

Mr. SELF. In the urban and rural environments, sir, it is, in all three environments, it comes down to the proper mix, and the proper mix is, of course, personnel, it is infrastructure and technology. In urban and rural, we have minutes to seconds to respond, especially in the urban environment. The smuggling infrastructure in the urban environment is normally directly adjacent to the international fence or the international line. If we don't have the infrastructure, the fences, the individuals penetrating the border can come in and be within the smuggling infrastructure and heading into the interior of the United States within minutes to seconds. Therefore, we need the infrastructure.

In addition to that, typically, in our urban environments, we do have technologies. We have RBSS cameras that survey the fence. In some areas, we have attended ground sensors that will pick up somebody walking into the United States. There is a mix of tactical infrastructure and technologies in our urban areas. For the most part, however, it is not clear across the border at this time.

Mr. MITCHELL. Thank you. I now recognize Mr. Hall for five minutes.

Mr. HALL. Thank you, Mr. Chairman. Chief Self, I probably owe you an apology. I called you a general when I was out there earlier. I saw those two stars there. You have a lot heavier duty and more territory to cover than an average general does. You are the division guy out of a great area.

Mr. SELF. Yes, sir.

Mr. HALL. Very valuable to us.

Mr. SELF. Thank you, sir.

Mr. HALL. And I would like for you to hurry up with your testimony and get on back to doing what you are doing, because we need you.

Mr. SELF. I would rather be out there than here, sir.

Mr. HALL. Yeah, I know you would. And I will correct something on you, Dr. Hooks. By golly, you are a doctor, because I looked in the dictionary, and it says a doctor is a learned person, and you taught me all about these exhibits here, that I know more now than most citizens do, and I can answer a lot of questions that I get asked.

Mr. HOOKS. Thank you, sir.

Mr. HALL. I don't know how I am going to fully describe all that, but I am just going to tell them we have it, and they will have to take my word for it.

I mentioned in my opening statement, Dr. Jackson, about the fact that you tracked a number of terrorist groups, and that you had some good advice about our need for a multi-layered defense. Do you want to enlarge on that a little?

Dr. JACKSON. Sure. I mean, in the work that we did, we looked across the whole world. So, we picked terrorist groups from—everyone from the LTTE in Sri Lanka, which is a very structured and well researched terrorist group, to Jemaah Islamiyah in Indonesia, and we did that because we wanted to cover the variety of the threat that technologies face from groups responding.

And in looking across that, what struck us was the commonality in the ways that a lot of these groups sort of came at the defenses that were put in their way, because technologies can be—provide a very potent security role, they are something that are threatening to the interests that the terrorist groups are trying to advance, so they respond to them.

And so, in thinking about a multi-layered defense, and one element of that is sort of the multi-layers that we have heard here, you know, talking about reinforcing the fence with sensing equipment, so you have, you know, multiple layers at the same time. But the other element of this multi-layer idea that came out in our research is this idea of making sure that we have a portfolio of technologies available, not that we are all using at the same time, to provide multi-layers right now, but also we have things on the bench, if you will, to roll out if the first layers are broken through. And so, it is a multi-layered defense not just at the same time, but providing our ability to reconstitute the layers of our defense over time, because of course, as I am sure anyone who does this on a day to day basis knows, this is an ongoing, long-term contest between the people who are trying to break through the border, and the security organizations that are trying to keep that line.

And so, as a result, we have to be prepared to think about what we are doing, and the benefits of what we do over the long-term.

Mr. HALL. Getting back to you, Mr. Hooks—Dr. Hooks. In your testimony, you state that tunnel detection is an example of research the Directorate likes to tackle through the basic research portfolio for Fiscal Year 2009. What specific programs are you seeking funding for, for Fiscal Year 2009, and where would these be carried out?

Mr. HOOKS. Specifically related to tunnel research?

Mr. HALL. Yes. Yes, and that's in this bill.

Mr. HOOKS. We are looking to pursue specific efforts in fiber optic technology and enhancements, so that they could detect when tunnels are being built, the vibrations of the tunnels being constructed, and/or the people passing through them.

Mr. HALL. Just give us an idea about what kind of problem tunneling is.

Mr. HOOKS. Problem——

Mr. HALL. Yeah.

Mr. HOOKS. Problem from a detection standpoint?

Mr. HALL. Detection, prevention. The length of the tunnels. What is the longest tunnel you have ever seen?

Mr. HOOKS. I can't specifically comment on——

Mr. HALL. But can you come close to it?

Mr. HOOKS.—on the details.

Mr. HALL. I have heard that they have been, tunnels as far as a block.

Mr. HOOKS. Oh, at least a block. In different locations, and Chief Self can probably provide some specific details.

Mr. HALL. I will ask the Chief about that.

Mr. SELF. That is correct, sir. We have had tunnels as far as several hundred yards, starting in Mexico, and tunneling into the United States.

Mr. HALL. And how do you detect—how can you detect that? How far underground is the tunnel?

Mr. HOOKS. Tunnels aren't that deep, 20 yards or so. I am sure there are cases they have been deeper.

Mr. SELF. One problem they have in tunneling, sir, is they have to deal with the water level in certain areas of the Southwest border. Therefore, in some areas, you can have them as deep as 12, 15, 20 feet. In other areas, they are only anywhere from six to say, eight, 10 feet below the surface.

Mr. HALL. Go ahead and answer the question I asked you a moment ago.

Mr. HOOKS. Yes, sir. And so, the challenge in tunnel detection is being able to detect it in near real time. Ideally, to support their operations in a nonobtrusive manner and quickly, using some kind of different detection scheme, whether that be looking at the vertical deflections, gravity deflections, electromagnetic deflections or whatnot, and right now, the equipment is just not sensitive enough, so that you could fairly rapidly, maybe using a truck at the border going 10 miles an hour along the border, be able to detect a tunnel successfully, not receive a lot of false positives, so that the Border Patrol could then take, excuse me, corrective action accordingly.

Mr. HALL. I think my time is up. Mr. Chairman, are we going to be allowed to send questions to them?

Mr. MITCHELL. Yes, we will.

Mr. HALL. Okay. I thank you for my time, and I am sorry I went over the time.

Mr. MITCHELL. I thank you. At this time, I recognize Ms. Richardson for five minutes.

Ms. RICHARDSON. Thank you, Mr. Mitchell.

First of all, I would like to take a moment to commend Congressman Hall for bringing forward this legislation, H.R. 3916. I think nothing is more important when we talk about setting appropriate priorities, particularly having to do with research and funding, taxpayer funding that is going towards this, that it is done in the right way.

So, congratulations, Congressman Hall, on your efforts today. I simply have one question for Mr. Hooks, and that is, when technology is developed by the Department of Homeland Security's Science and Technology group, how is it that a technology's performance is validated?

And let me preface what I am saying to give you an example. I represent Southern California, and we recently had a spill in Northern California, where you know, a bridge was hit, and oil was dumped, and the Coast Guard was supposed to have been there, and you know, first of all, they shouldn't even have run into the bridge to begin with, then oil was dispersed into the water. No communication was made to the public for eight years. It was just a comedy of errors, and when I say comedy, I don't mean it in a humorous way. It was a disgraceful way, in my opinion.

So, I am concerned with the tremendous amount of funding that we use to, you know, utilize these technologies to protect our borders, but sometimes actually validating the performance of all this work is where we have a shortfall.

So, if you could tell us a little bit about what your department is doing in that aspect, and how you work with other groups or independent agencies to assist us in this effort?

Mr. HOOKS. Yes, ma'am. It is important, we totally agree, to effectively test the technologies before they are placed in an operational environment with the different components. To do that, we use several different means. Underneath each of the Capstone IPTs, we have created project IPTs, where program managers from the components, such as the Border Patrol, and program managers in S&T, are coming together with appropriate end-users, and defining the specifics of that equipment, the requirements that it needs to meet.

Commensurate with that, they also need to define what are the appropriate test and evaluation procedures that should be followed, testing of that equipment both in the laboratory setting and out in an operational setting, so that by the time that equipment is transferred to the Border Patrol for procurement, they can be confident that it works correctly.

So, we would encourage them, and surely, they would participate in that evaluation of the testing of the equipment as we go forward, so that they can feel confident at the point that they receive it that it works properly. One example is we have a test bed down at the

Southwest Border at Douglas, where we take new technologies down there, we give them to the Border Patrol agents. Our Science and Technology people will be there, but they are using them in the background of their normal day-to-day operations, giving us feedback on it, and helping us to evaluate the equipment, to make sure that it is operating effectively.

Ms. RICHARDSON. And when you say they give you feedback, are these the actual ground patrol officers who are providing you with the results?

Mr. HOOKS. Yes. Yes, down in the Tucson sector, either the Sector Chief, his specific agents, he has a component down at the Douglas Test Site that specifically engages with us. These are Border Patrol agents in that sector that are using the technology, and we get direct feedback from them.

Ms. RICHARDSON. Thank you, Mr. Hooks. I yield back my time, Mr. Mitchell.

Mr. MITCHELL. Thank you. I now recognize Dr. Gingrey for five minutes.

Mr. GINGREY. Mr. Chairman Mitchell, thank you very much, and I want to thank all of the witnesses for being here this morning, and this is a hugely important issue. We all know that, and not only our ground borders, but maritime security, we haven't talked too much about maritime, but I have certainly had the opportunity to go to the Southwestern border. We are talking about 2,000 miles, aren't we, Chief Self?

Of course, the Canadian border, it is a longer border, but I think our main focus, at least, on the Southern border, is paying great benefits. Chief, I commend you for your long service there. I actually went to Nogales, and we saw some of the work of your people on the ground in the heat of the day, and the dark of night, 24/7, doing their work, and I want to commend you and, of course, everybody else on the panel, for being here, and helping us understand a little bit better. I'm proud to be a co-sponsor of Mr. Hall's legislation.

And I wanted an answer to a couple of specific questions, and actually, the first one, Mr. Kapos, is in regard to HSSTAC. I understand there was a lapse of authorization for HSSTAC back in 2006, and I want to know, did that adversely affect the S&T Directorate's ability, their organizational and planning capability, when that authorization was not forthcoming in 2006?

Could you comment on that for us?

Mr. KAPOS. Sure. I was not there, but all the same, I got to pick up the pieces. By the time the HSSTAC was reauthorized, we had only six members of the original 20.

Mr. GINGREY. Of the original 20, did you say?

Mr. KAPOS. Yeah. Yeah.

Mr. GINGREY. Describe these 20 people.

Mr. KAPOS. Well, they are representatives of scientific disciplines, and of the first responder community, who had an interest in—obviously, first responders have an interest in, but the scientists are specifically picked to be people who are eminent in their fields, and to have an interest in homeland security problems.

As I said, by the time the HSSTAC was reauthorized, there were only six of them left, whose terms had not either lapsed——

Mr. GINGREY. Six out of 20?

Mr. KAPOS. Yeah. Whose terms had not either lapsed or who had not resigned in order to accommodate other commitments. And actually, it turned out to be fairly straightforward to recruit 14 people, because by and large, the people that I contacted came from lists that had been prepared previously of people who were interested. And by and large, they were very willing, but we have to face up to the fact that the HSSTAC didn't meet for the best part of a year, and it took us about two or three months to get the people recruited and screened and so on.

We had our first meeting in late August in Newport, and we meet again in December in Arlington, and in between these two meetings, we have had a number of fact-finding meetings. We have been working pretty hard. As a result, while you would like not to lose any momentum, it turns out to be less problematic than it might be to regain it.

Mr. GINGREY. Well, we appreciate your strong effort in restoring to that 20 number, and trying to replace those 14 who were so valuable. My five minutes went mighty quick, I guess, this slow, Southern way of talking. But let me just follow up. I have got a few seconds left and may as well stick with Mr. Kapos, in regard, how was the current task of IED threat assessment chosen, if you could discuss that with us in the brief time we have left?

Mr. KAPOS. Yes, indeed. The Under Secretary has been very concerned about the need to prepare for this threat. Now, IEDs, coming to a theater near you. And he was, in particular, concerned, that there was not a properly rounded program to address this. Running across the kill chain, from indication and warning, from prediction, from detection, all the way through to response. So, he simply asked the HSSTAC to look at it from that viewpoint, and I must say, since I get to sit through every endless meeting with the HSSTAC, that they are doing a very, very good job of considering the entire spectrum.

Mr. GINGREY. Thank you very much, Mr. Kapos. Hopefully, we will have a second round, and I can address some questions to the other witnesses.

Mr. Chairman, I yield back, and I thank you.

Mr. MITCHELL. Thank you. My understanding is we are going to be called to votes in about 10 minutes, so at this time, I would like to call on Mr. Wu, and then, we will call on Mr. Smith.

Mr. WU. Thank you, Mr. Chairman. And I am going to ask a question. I am going to ask two questions, and I will take the answers in writing. If we have time, we will take them here in the Committee, and then, I would like to focus on a third question.

And the first piggybacks on Mr. Hall's question about tunneling, and also, gets at the issue of long-term versus short-term research. And with respect to tunnel detection research, it was pointed out that there are some basic research investments which are needed as a first step, and yet, the S&T Directorate is awarding a contract for shorter-term tunnel detection technology, and I am a little bit troubled that while the foundation might not have been laid, that we are charging ahead with short-term technology, and I am concerned that that would lead us to wasted research.

And I would like the Department to justify awarding the short-term contracts, while the basic research hasn't been done yet. And maybe there is a good explanation for that, and maybe there isn't.

Now, we will jump from underground to overhead, and I would like to know what the biggest technological challenges are in the UAV R&D area. Who is responsible for performance testing the UAVs? What criteria does the Department use to develop UAVs and define successful operation of UAVs, and I will take answers to both those questions in writing unless we can get back to it. This five minutes goes really fast.

Now, Mr. Kapos, about HSSTAC, I am very concerned about long-term research versus short-term research, and laying the foundation in long-term research, so that, you know, we are not firefighting all the time, and you know, we do have to do a certain amount of firefighting in response to immediate threats. But you know, the challenge, and I think the challenge for the S&T Directorate, has always been that there is concern that you all are short-sighted. There has been too much focus on short-term stuff, and not enough foundational work, so that we have the flexibility to flex with the changing threat environment.

And the concern is that the one tool, or a very important tool for setting long-term priorities is HSSTAC, and yet, that is a tool that has now been very strongly focused on IEDs, which is the threat of the day, and so, the problem is we have a problem with short-sightedness, and now, you have just taken the glasses off. We have gotten every more shortsighted, because HSSTAC has been focused on a near-term threat rather than looking out there, and appropriately setting priorities for the S&T Directorate's long-term research.

Can you respond to what the S&T Directorate is doing about the long-term, while appropriately addressing the short-term, and whether HSSTAC has been hijacked to, you know—into short-term projects?

Mr. KAPOS. Sure. First, let us address the IEDs, because the HSSTAC is looking explicitly at IEDs in the farther future, five and more years into the future, and——

Mr. WU. Now, what about non-IED threats? Shouldn't we be concerned about those also?

Mr. KAPOS. Most certainly, we should.

Mr. WU. I mean, you know, there are broad categories, you know, things like biosecurity, cyber security, et cetera. I mean, you know, folks don't just focus on one thing.

Mr. KAPOS. No, no. I agree. When we finish our consideration of IEDs in the five- to 10-year future, which will be about the 1st of February, then will be the time to pick another problem. And certainly, cyber security is begging for a look. Certainly, biosecurity is, too. But it is important, I think——

Mr. WU. HSSTAC is configured to just handle one thing at a time?

Mr. KAPOS. It is, pretty much. There is nothing that says that we cannot subdivide the HSSTAC and consider two problems or three problems, but remember, please, that the law allows for only 20 members, and so we have to worry about having a sufficient

concentration of the various disciplines in order to provide a well-rounded consideration.

Mr. WU. Well, how many JASONs are there in the JASON program at DOD? I mean, aren't they supposed to look at a universe of defense threats, and that is sort of their task? And why is HSSTAC different from that?

Mr. KAPOS. I cannot answer why HSSTAC is different from that. I don't know how many JASONs there are, but I do know that the JASONs lay out a study program for themselves a year ahead, and they go from problem to problem to problem. And that is pretty much what we are trying to do with the HSSTAC.

Mr. WU. Except in this instance, HSSTAC didn't pick IEDs themselves, they were told to do so.

Mr. KAPOS. Well, there was considerable consultation between the Under Secretary and the Chairman of the HSSTAC before they settled on IEDs. And as I say, the IEDs are crying out for an integrated, broader spectrum program than they have had in the past. So, I guess I am saying that I don't quite agree that it has been hijacked by the immediacy of the problem.

Mr. MITCHELL. Thank you. I would like to now recognize Mr. Smith.

Mr. SMITH. Thank you, Mr. Chairman.

Mr. Hooks, if you wouldn't mind answering this question. A 2008 budget request for the Border and Maritime Division is only about three percent of the total S&T budget. Can you elaborate on why that would seem, at least on its face, to be such a small amount? As a percentage of the entire budget? Or of the Directorate's activities, at least?

Mr. HOOKS. Excuse me. I can say that within our S&T budget, in my particular area, in the transition area, we look at the 11 different functional areas that we have broken down the DHS mission space to, and with the leads of the different components, they have identified what their highest priority gaps area that require technology solutions. We propose different technology programs and cost estimate them to provide those solutions.

And then we have created a Technology Oversight Council that is led by the Deputy Secretary of the Department, where he looks, in an integrated fashion, across those 11 IPTs and the requirements of each of those 11 IPTs, and based on risk in those functional areas and his considerations, he is charged with the balancing of that effort to make sure that it is meeting across the spectrum of effort the highest-priority needs of the Department. And that is how that budget is formed.

Mr. SMITH. Okay. Thank you. I yield back.

Mr. MITCHELL. Thank you. Before we bring the hearing to a close, I want to thank our witnesses for testifying before us today.

The record will remain open for additional statements from the Members, and for answers to any follow-up questions the Committee may ask of the witnesses.

The witnesses are excused, and the hearing is now adjourned. Thank you.

[Whereupon, at 11:16 a.m., the Subcommittee was adjourned.]

Appendix 1:

Answers to Post-Hearing Questions

ANSWERS TO POST-HEARING QUESTIONS

Responses by Robert R. Hooks, Director of Transition, Science and Technology Directorate, Department of Homeland Security

Questions submitted by Chairman David Wu

Q1a. What are the biggest technological challenges in the area of unmanned aerial vehicle (UAV) R&D? Who is responsible for performance testing for UAVs? What criteria does DHS use to define successful operations for UAVs?

A1a. The biggest technological challenges DHS faces today in Unmanned Aerial Vehicle (UAV) R&D involves: Fulfilling FAA requirements to operate within the National Airspace System (NAS), expanding sensor capabilities allowing DHS to discriminate criminal activities at medium- to high-altitude operating regimes, and maximizing the operational benefits of an unending stream of data information obtained by sophisticated UAV platforms.

- In order to have the FAA allow DHS unmanned aerial systems (UAS) into the National Airspace System (NAS), they currently require a lengthy approval process to fly in a very controlled and confined environment. The FAA will become much more flexible once they can be assured of collision avoidance between UAS' and manned/other unmanned aircraft. To accommodate this requirement, automated sense-and-avoid systems, capable of detecting and sidestepping oncoming aircraft without a pilot's intervention are required to assure collision avoidance. The challenge to accommodate this provision lies in the fact that the avoidance system must be fully automated without human intervention as one would find in manned aircraft.
- In order to take full advantage of increased surveillance opportunities found with advanced UAS capabilities—altitudes from 18,000 to 65,000 feet and longer station times of up to seven days—UAS payloads and sensors need greater sensitivity and resolution to meet DHS requirements. Requests for such complex UAS platforms have pushed the envelope for producers of sensor equipment because the demand for such high-resolution/high-sensitivity sensors (i.e., sensors that can optically discriminate features of illegal cargo and people engaged in illegal activities) is relatively new. DHS' ultimate goal is a UAV platform that yields a fully functional operating picture that highlights areas of potential criminal activity.

Q1b. Who is responsible for performance testing for UAVs?

A1b. DHS is exploring options for performance testing providers. Until a final determination can be made, DHS is working through cross-organizational and cross-agency venues to conduct performance testing. For example, DHS partnered with DOD for one DOD UAS-related Joint Concept Technology Demonstration. DHS also has planned the UAS Gulf Coast Demonstration (GCD) to determine acceptable platform and sensor performance. This particular demonstration will combine the operational efforts of multiple DHS Agencies while using the test and evaluation capabilities of the Science and Technology Directorate.

Q1c. What criteria does DHS use to define successful operations for UAVs?

A1c. The criteria that DHS uses to define successful unmanned aircraft systems (UAS) operations are availability, mean time between failure, mishap rate, etc. Customs and Border Protection (CBP) is the operator of UASs within the Department and establishes these criteria. CBP tracks statistics for law enforcement operations such as the number of apprehensions made or pounds of illegal drugs confiscated. UAV performance is measured against metrics based on these statistics.

Q2a. With regards to tunnel detection research, you point out that basic research investments are needed as a first step towards developing effective tunnel detection technology. Yet you also say that DHS S&T is awarding a contract for a shorter-term tunnel detection technology effort. What is the goal for developing prototype detection technology, given that much of the important foundation research has not yet been conducted? How much is DHS S&T spending on this High Impact Technology Solution (HITS) project?

How will DHS S&T test and validate any technology developed through this HITS project? If the technology is successful, what steps will DHS take to make this technology available to CBP? What criteria, outside of technological capabilities, will DHS use to measure success? Cost? Training requirements?

A2a. The *Homeland Security Act of 2002* calls for the Homeland Security Advanced Research Projects Agency (HSARPA) to "promote revolutionary changes in technologies. . ." In the execution of that direction, the S&T Directorate's Innovation/HSARPA work pursues technologies that have potential to achieve results far sooner than the normal development process. The Tunnel Detection effort is one of the S&T Directorate's High Impact Technology Solutions (HITS) projects, where we invest a relatively small amount of money, accepting considerable risk of failure, in order to pursue a potential proof-of-concept answer within one to three years. This approach challenges industry to think outside-of-the-box and to develop leap-ahead technologies. However, because of the potential risk of failure of this approach, it is important that this work takes place in parallel with more conservative approaches, including longer-term, basic research.

Q2b. How much is DHS S&T spending on this High Impact Technology Solution (HITS) project?

A2b. The S&T Directorate FY 2007 budget for the tunnel detection HITS project is $2 million. The S&T Directorate's planned FY 2008 budget for the tunnel detection HITS project is $1 million.

Q3. In your testimony, you discuss the S&T Directorate's plans for tunnel detection research. Specifically, you say you "intend to study and characterize the geophysical characteristics of key border regions," beginning in FY 2009. Why do you believe DHS should carry out this research, as opposed to the U.S. Geological Survey? More generally, how do you determine whether DHS should carry out certain research as opposed to agencies with greater expertise in specific fields?

A3. The Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) agencies are partnered with the S&T Directorate to develop and demonstrate robust and reliable tunnel detection technologies. In support of this effort, we will review U.S. Geological Survey data to determine the existing geophysical characteristics of a region-of-interest. Such data is important to enabling the technology to detect anomalies or changes that would indicate the existence of a tunnel.

Q4. In your testimony, you discuss current cargo security research efforts. How has DHS engaged with end-users of these technologies, such as shipping industry representatives, to develop performance requirements and standards for tracking and cargo identification technologies?

A4. The S&T Directorate's Borders and Maritime Security Division uses a variety of methods to engage industry on the development of performance requirements and standards for emerging tracking and cargo-identification technologies. These include industry forums, requests for information, and one-on-one discussions with container and maritime industry representatives.

For example, the S&T Directorate meets regularly with members of the shipping industry. Through dialogue with several ocean carriers, we found that two of the systems developed by our office, the Marine Asset Tag Tracking System (MATTS) and the Hybrid Composite Container, could provide broader commercial benefits in addition to our intended security objectives. MATTS can provide efficiencies from improved asset visibility, while the Hybrid Composite Container offers more durability and weight savings over existing containers. Industry could benefit commercially from the potential promulgation of cargo security standards such as these. Additionally, the S&T Directorate continues to seek and has received the cooperation of the shipping industry to test these technologies.

The S&T Directorate also uses industry forums and invitational speaking engagements to ensure a broader outreach across carriers and shipping industry end-users. Recently, in November 2007, we addressed the annual world-wide Terminal Operators Conference (TOC) in Panama on the S&T Directorate's Cargo Security Program. During this review, we received positive feedback on our approach to solving complex security issues involving container shipping.

The S&T Directorate has met with the World Shipping Council and members of the Department of Transportation (DOT) Supply Chain Security Working Group to discuss the role of standards in both industry and government related to cargo and shipping containers. The S&T Directorate is supporting the U.S. Customs and Border Protection (CBP) Working Group focused on cargo and container security standards. CBP is the United States' representative to the World Customs Organization (WCO). International standards would need to be promulgated through the WCO, as the end-user regulatory body, through their SAFE Framework of Standards.

Questions submitted by Representative Ralph M. Hall

Q1a. During the hearing you described the process by which the Deputy Secretary looks across the 11 IPTs to determent funding priorities for the Directorate. What information does the Deputy Secretary use to determine the relative investment among the IPTs? Similarly, what metric does S&T use to determine what projects are funded in the high-risk, Innovation portfolio?

A1a. The Deputy Secretary has established a Technology Oversight Group (TOG) to provide oversight of the S&T Directorate's Capstone IPT investments. The TOG is chaired by the Deputy Secretary and consists of the DHS Under Secretary for Management and the DHS Under Secretary for National Protection and Programs. The DHS CFO attends, and the DHS Under Secretary for Science and Technology is the Executive Secretary. Through the TOG, the Deputy Secretary provides oversight of the S&T Capstone IPT investment and ensures investment balance across the Capstone IPTs. In implementation, the DHS Under Secretary for Science and Technology provides the Capstone IPT-approved, -prioritized and -recommended S&T Enabling Homeland Capabilities (EHC) to the TOG. The TOG validates the customer focus and ensures that proposed S&T Directorate programs support Department-wide strategies and concerns.

The TOG prioritizes funding across S&T Directorate Divisions using specific criteria such as:

- Magnitude of Vulnerability/Risk—projects that would significantly reduce the known vulnerability/risk to a known threat;
- Projects that address one or more of the DHS priorities identified;
- Cross-cutting Department priority—projects that address high-priority capability gaps identified by multiple IPTs;
- Ability to fill a major capability gap—projects that have a high potential to fill a capability gap identified by IPTs;
- Transition timing—projects that match transition with a scheduled DHS acquisition program upgrade; and
- Expected delivery time.

Q1b. Similarly, what metric does S&T use to determine what projects are funded in the high-risk, Innovation portfolio?

A1b. The initial (current) set of Homeland Innovative Prototype Solutions (HIPS) and High Impact Technical Solutions (HITS) projects were selected in early FY 2007, prior to the initial meeting of the S&T Directorate's Capstone Integrated Product Teams (IPTs). They were selected as a result of the Under Secretary for Science and Technology's participation in a two-day off-site with all Department leadership. The Under Secretary was able to identify the priority gaps in capability as described by leadership and those gaps became the initial HIPS and HITS. The list of HIPS and HITS projects has been extremely well received by our customers and has generated tremendous interest among industry. New HIPS and HITS will be selected from various inputs including the IPT process, unsolicited input from industry and laboratories, and from teaming opportunities with other agencies. The S&T Directorate's Corporate Board will review all potential candidates for HIPS and HITS categories and make final program decisions.

Q2. In your testimony you describe a UAV simulation S&T is currently developing with the FAA. How will this simulation help ease the barriers to regular operations of UAVs in the National Airspace System? Will S&T also pursue flight tests of relevant safety hardware?

A2. Unmanned Aerial Vehicles (UAV) simulation between the S&T Directorate and the Federal Aviation Administration (FAA) will directly affect the relationship during regular operations of UAVs in the National Airspace System (NAS). By coordinating during the simulations, the process of putting more UAVs in the NAS will be much safer. Simulations will address issues such as the airspace during take-offs and landings as well as in-flight collision avoidance. Since many UAVs fly at the same altitude as manned aircraft, this is where most of the coordination is needed. By doing simulations that will practice take-offs and landings and flying in the vicinity of manned aircraft, DHS organizations and the FAA will help ease the barriers during regular operations as well as last-minute disaster relief operations such as the recent wildfires in California. By preparing emergencies during simulations, DHS organizations as well as the FAA will be able to coordinate and manage the NAS much more efficiently.

The S&T Directorate is working with the FAA and DOD to pursue flight tests of relevant safety hardware including collision avoidance systems. The fact that UAVs are unmanned makes safety in the NAS the highest concern to the S&T Directorate, and we intend on ensuring all relevant safety hardware has been properly tested and standardized.

Q3a. Dr. Jackson's testimony highlighted the need for regular red-teaming to ensure technological defenses cannot be immediately overcome. What role does red-teaming play in current testing and R&D activities of the Directorate? Dr. Jackson also spoke about the potential need for organizational changes to utilize new technology or adapt to opponents. Does the S&T Directorate have the expertise to advise DHS components on organizational or operational improvements or provide research in this area?

A3a. The S&T Directorate agrees with the importance of red teaming and is evolving an external red team capability. Within the S&T Directorate, we look to various laboratories to provide red teaming capability on selected technologies.

Q3b. Dr. Jackson also spoke about the potential need for organizational changes to utilize new technology or adapt to opponents. Does the S&T Directorate have the expertise to advise DHS components on organizational or operational improvements or provide research in this area?

A3b. The DHS operational components are the experts in their operations and organizational structure. The S&T Directorate will closely coordinate with the operational components on the development of incremental and innovative technologies. Through this close coordination, the operational components will be better able to evaluate these technologies, evolve new concepts of operations if necessary, and determine the degree of operational improvement each technology provides. This close coordination manifests itself through the Capstone IPT process where the S&T Directorate develops a better understanding of operational requirements. Demonstrations and pilots of technologies allow operational components and end-users to better understand and evaluate the technology as it matures, and experimentation provides an environment for the operational components to test the edges of the technology and the underlying operational concepts. The S&T Directorate is a component of this important chain, but our operational customers are the experts and end-users.

The S&T Directorate has developed various test beds to evaluate technology in actual operational environments. The test beds allow us to evaluate technology for survivability, operational efficacy, and susceptibility to counter-measures. Relevant to Border Security, our border test beds provide integrated system level test platforms for evaluating border security sensor and processing technologies and demonstrating their performance in an operational environment. Furthermore, the test beds mature those technologies for transition, reduce associated technology risk, and establish lessons learned for our operational components. For example, in FY 2006, the S&T Directorate installed a southern border test bed in the Tucson sector of Arizona, which tested Border Patrol officer's abilities to remotely access databases, sensor alerts, and geo-spatial information via vehicle-mounted computers and hand-held devices. In FY 2007, the S&T Directorate expanded the southern border test bed by extending access to multiple law enforcement databases; deploying an in-field, 10-fingerprint reading system; improving radio direction finding of individuals conducting counter surveillance in support of illegal activity; and adding a law enforcement asset location tracking capability (blue force tracking). In FY 2008, the S&T Directorate will install a northern border test bed demonstration in the Swanton sector of Vermont, which will include a multi-sensor fusion function, field level scene awareness capability, and law enforcement data base query. This puts new technology in real-world environments against real-world adversaries and provides a measure against current operational technologies and capabilities.

Q4a. In your testimony you describe the university-based Centers of Excellence (CoE) as an integral part of the Directorate's long-term research agenda. How much of the Directorate's basic research is performed through CoE's versus individual grants or national laboratories? Does the Directorate have a planning mechanism for long-term research across all of the divisions?

A4a. About 50 percent of the S&T Directorate's basic research budget goes toward Centers of Excellence (CoE) research.

Q4b. Does the Directorate have a planning mechanism for long-term research across all of the divisions?

A4b. Yes, the S&T Directorate develops long-term research programs with the divisions. Long-term research develops the fundamental or scientific technical basis or understanding that future systems and devices will be based on. Long-term research needs are derived mainly from three sources; basic or fundamental research issues that are identified in the IPT program planning process, priorities unique to Homeland Security solutions, and leveraging opportunities with our research partners that have strong Homeland Security applicability. The S&T Directorate coordinates basic research workshops between the divisions and DHS in-house labs, the National Laboratory networks, and the CoEs.

Q5a. To the credit of Under Secretary Cohen and yourself, the Integrated Product Team (IPT) process has significantly improved S&T's responsiveness to the other components of DHS. Does the focus on technologies that can be delivered in three years or less, however, bias the Directorate towards modest changes of existing systems? Is the IPT review system capable of assessing long-term research goals?

A5a. No. The Capstone IPT process is only one pillar of the S&T Directorate's investment effort. We also recognize the need to invest in basic research and in higher risk innovative technologies. The three S&T Directorate investment pillars compliment each other by allowing S&T to address near-term capability gaps while investing in longer-term solutions. The focus of the Capstone IPT process is to connect with the customer, understand their operations and capability gaps, and deliver near-term improvements to protect the Nation. Our innovation effort is informed by the Capstone IPT process but is focused on longer-term, higher risk, game-changing technologies. Basic research invests in areas where there are capability gaps but no near-term or innovative solutions. Basic research invests in these areas so that in the long run, we develop the understanding of the relevant basic science that will eventually provide the technical solutions our customers' need. Presently, about 15 percent of the S&T Directorate's budget goes toward long-term research. Our goal is to direct 20 percent of the S&T Directorate's budget toward long-term research.

Q5b. Is the IPT review system capable of assessing long-term research goals?

A5b. Yes, the S&T Directorate's IPT process provides the information that feeds long-term research planning. As our technical subject matter experts work with other DHS components, they identify many R&D needs. If a capability gap identified by the customer cannot be solved by a near-term technology solution, or an immature high-risk technology solution that is not evident, then basic research is necessary to advance the science and find breakthroughs that could result in future technology solutions. The S&T Directorate's subject matter experts (SMEs) work directly with DHS component representatives to determine which needs fit into the scope of the three-year target and through our innovation effort. Other long-term, high-priority needs identified during the process are handled through the office of the S&T Directorate's Director of Research.

Questions submitted by Representative Phil Gingrey

Q1. What were some of the capability gaps identified in the planning process CBP and S&T undertook? Were there projects that fell "below the line" and could not be immediately funded by the Directorate? If so, what were these items?

A1. Customs and Border Protection (CBP), along with Immigration and Customs Enforcement (ICE), co-chair the Border Security Capstone Integrated Product Team (IPT). The Capstone IPTs are arranged along departmental function lines, and thus, address overall border security and interior enforcement issues and not just a single component's priorities. As the co-chairs of the Border Security Capstone IPT, CBP and ICE followed a structured process that identified and assessed capability gaps. The Capstone IPT quickly realized that the high priority gaps identified by CBP were also common to ICE and the U.S. Coast Guard. The Capstone IPT identified several major acquisition programs that would benefit from the S&T Directorate conducting risk mitigation including CBP's SBINet and the U.S. Coast Guard's Command 21 programs. Additionally, capability gaps were identified in the following areas:

- Improved ballistic protection via personal protective equipment;
- Improved detection, tracking, and identification of all threats along the terrestrial and maritime border;

- Ability to access ICE databases in which voice information is entered; provide analytical, reporting, and automated case de-confliction; classify, and identify voice samples;
- Non-lethal compliance measures for vehicles, vessels, or aircraft allowing for safe interdiction by law enforcement personnel;
- Non-destructive tools to inspect hidden or closed compartments to find contraband or security threats;
- Improved analysis and decision-making tools that will ensure the development/implementation of border security initiatives;
- Ability to non-intrusively determine the intent of subjects during questioning;
- Ability for law enforcement personnel to quickly identify the origin of gunfire and classify the type of weapon fired; and
- Ability for law enforcement officers to assure compliance of lawful orders using non-lethal means.

There were capability gaps which fell below the line for the Border Security Capstone IPT based on resource limitations. The S&T Directorate's Capstone IPT process is customer-focused with the goal to deliver incremental technology improvements within three years. The three-year turnover establishes an automatic refresh capability. Once the Capstone IPT Process matures, we expect that each year 30 percent of our technology efforts will complete and transition, which would make funds available for the next below-the-line priority or the next, new, Capstone IPT-identified threat. The first priority Border Security Capstone IPT "below the line" capability gaps would be addressed by accelerating the following technology efforts: Tunnel Detection, Advanced Ground Surveillance Radar, Pattern Discovery and Prediction as a Decision Support System, Sense and Avoid Systems for Unmanned Aerial Systems (UASs), Counter Surveillance, and Less-Lethal compliance measures for personnel to provide solutions sooner to our DHS component customers.

Question submitted by Representative Adrian Smith

Q1. You mentioned in your testimony the Border Officer Tools program and explained how this program will enable border security and Coast Guard members to perform their current tasks more effectively and safely. Could you please explain in greater detail how these technologies are assisting border patrol officers on the U.S.-Mexico border?

A1. There are two main projects under the Border Officer Tools and Safety program in the Borders and Maritime Security Division: Border Officer Tools and Border Officer Safety. Border Officer Tools will improve law enforcement effectiveness and enhance officer/agent safety while searching vessels/vehicles. Many of these tools will leverage technology currently under development by either DHS or Department of Defense (DOD) for their purposes. One effort is developing tools that support secure communications (i.e., voice and data) between field operators as well as between field operators and their command centers. Another example is an effort to deliver intrusive (requiring contact) as well as non-intrusive, non-destructive technologies to aid in the identification of contraband. In FY 2009, the project will conduct a technology survey to identify documentation resolution versus bandwidth solutions to provide 24-hour, Real-Time Image Transmission of high-definition images and documents. The Border Officer Safety project will integrate technologies to enable border security law enforcement agents to perform their mission with greater safety. These technologies include, but are not limited to: Enhanced Ballistic Protection, Automatic Facial Recognition, Hidden Compartment Inspection Devices, and less-lethal Pursuit Termination-Vehicle/Vessel Stopping. In FY 2009, the project will develop and document ballistic vest performance requirements for border application, evaluate equipment/technologies and develop gun-fire location requirements for law enforcement agents.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Ervin Kapos, Director, Operations Analysis, Science and Technology Directorate, Department of Homeland Security; Executive Director, Homeland Security Science and Technology Advisory Committee (HSSTAC)

Questions submitted by Chairman David Wu

HSSTAC Format

Q1. The format of the HSSTAC was changed for the most recent iteration of the Committee. Previously, HSSTAC had a broad focus and provided recommendations for research priorities across the many fields covered by DHS S&T. Now, HSSTAC zeros in on specific project recommendations in a particular field, currently focusing on improvised explosive devices (IEDs). Why did the format of HSSTAC change? Given that the Committee is composed of experts from a variety of fields, are you taking advantage of the members' expertise when you focus on fields that fall outside their backgrounds? How does this format affect HSSTAC's ability to establish mission goals for the long-term?

A1. There have been changes to HSSTAC, however the Committee still adheres to its established responsibilities of reviewing and providing recommendations for research priorities across the fields that are, or possibly might be, covered in the programs of the S&T Directorate. In fact, that will be one of the topics to be covered in the next cycle of HSSTAC studies. At the same time, the Directorate asked the Committee to take intensive looks at problems that are pervasive in their impact on the S&T Directorate. For example, the HSSTAC will review what science and technology projects need to be undertaken in the next several years to provide an adequate basis for a capability to respond to the threat of improvised explosive devices (IEDs) in the U.S. domestic environment. Members of the HSSTAC have worked on the various portions of this problem as their backgrounds and expertise have particularly qualified them to do. The Committee also meets as a whole to critique and integrate the partial answers to the problem which becomes broad ranging advice to the Under Secretary for S&T. Finally, members representing the various academic disciplines have integrated well with the members representing the various first-responder and related fields, and we have found that this mode of operation supports HSSTAC's capability to establish mission goals for the S&T Directorate.

HSSTAC Expertise

Q2. Does the membership of the HSSTAC include operational expertise that would allow the Committee to inform the Directorate on tactical concerns such as concepts of operation or organizational issues within the Directorate or other DHS components?

A2. Yes, the membership of the HSSTAC includes the operational expertise required to allow it to advise the S&T Directorate on concepts of operation and organizational issues that arise. Nearly all of the members have broad ranging and deep experience in Homeland Security activities and in what has been found to work and not to work in these areas in the past. Also, the membership includes representatives of the first-responder communities, such as law enforcement, fire safety, emergency management, and health affairs. The interaction between these first responders and the representatives of the various scientific disciplines on the HSSTAC has been consistently productive of valuable insights in areas such as concepts of operation and organizational issues.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Brian A. Jackson[1], Associate Director, Homeland Security Research Program, The RAND Corporation

Questions submitted by Chairman David Wu

Q1. In your testimony, you said, "the effectiveness of security technologies can degrade as our adversaries adapt and alter their behavior in response to the introduction of defensive measures. That adaptive behavior can pose a significant risk to the security benefits new defensive technologies are intended to provide and, therefore, must be considered in technology planning." In your opinion, does DHS S&T recognize the need for adaptive, flexible technology planning? How do the contributions of various advisory groups, such as Integrated Product Teams and the HSSTAC affect DHS S&T's ability to adapt to new challenges?

A1. Our research on the effects of terrorist adaptive behaviors on the efficacy of defensive measures was sponsored by DHS S&T's Office of Comparative Studies to identify the implications for S&T planning for combating terrorism. Because RAND has not had the opportunity to examine DHS S&T's technology planning processes or the activities of groups like the Integrated Product Teams and the HSSTAC, I unfortunately cannot provide an informed answer on the extent the ideas developed in our or others' work on this topic are reflected in DHS planning efforts.

Q2. You specifically mention how adversaries have been able to defeat the technologies identified as priorities in the bill: unmanned aerial vehicles (UAVs), tunnel detectors, and anti-counterfeit technology. How should these identified vulnerabilities affect how DHS proceeds in these research areas?

A2. Terrorist groups' past efforts to degrade the effectiveness of priority technologies like UAVs, tunnel detectors, and anti-counterfeiting technologies can inform research planning in two ways.

First, the ways that terrorist groups have found to do so provide lessons for improving future technologies that can be directly applied in current research activities. If approaches can be devised that render terrorists' past counter-technology strategies ineffective, our future defenses will be stronger as a result. Our research has shown that responding to terrorist adaptive behavior can involve modifications to the technical systems themselves, which would need to be an integral part of R&D programs, but frequently require changing the concepts of operation for how technologies are used as well. This emphasizes that in developing new defensive measures it is important to consider the ways those technologies will be used as part of the development process, since those concepts of operation may be critical to maintaining the technologies' effectiveness. It also underscores the importance of the transition efforts to move new technologies to end-users and help shape their application.

Second, in designing research programs for these priority technologies, the principles identified in our research and summarized in my testimony are important to ensure that the defensive measures we develop in these areas are robust to adversary adaptive efforts. Including testing, red teaming, and small scale technology pilot efforts in R&D programs is needed to identify and address vulnerabilities to their effectiveness. Furthermore, given that adversary groups have shown remarkable flexibility to respond to even sophisticated technologies, it is also critical to maintain reasonable flexibility in the technologies being developed and to build R&D portfolios in each of these areas (i.e., rather than focusing on only a single technology choice) to preserve "fall back" defensive options if the effectiveness of deployed technologies is compromised.

Questions submitted by Representative Ralph M. Hall

Q1. What assessment technique would you suggest for determining the funding priorities among threats such as border security or radiological detection?

---

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of the RAND Corporation or any of the sponsors of its research. This product is part of the RAND Corporation testimony series. The series records testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

A1. In RAND's past research and testimony on homeland security, we have advocated that funding priorities should be informed by risk analysis—an assessment of the threat of specific attacks, the vulnerability of targets of concern to those attack modes, and the consequences that would occur if an attack was successful. Use of risk analysis in policy planning ensures that priorities are defined not just by one these three factors in isolation but by all three together, providing a way of considering high probably, lower consequence events—such as "everyday" illegal border crossings by individuals—with lower probability but potentially higher consequence events—such as radiological material being smuggled into the country.

A risk-informed priority setting process for R&D would consider the seriousness of individual risks and select technology priorities and options based on their ability to reduce those risks. The results of our research on terrorist responses to defensive measures could contribute to such a process since those responses degrade the effectiveness of defensive technologies, thereby cutting their ability to reduce risk.

Q2. What implications does your research have for the appropriate balance between short-term and long-term research projects? Are incremental changes to technological defenses enough to stay ahead of opponents' counter-efforts?

A2. It is difficult to provide a general answer to whether incremental, short-term technological changes are enough to stay ahead of adversary adaptive efforts. For some technologies, incremental efforts may make it possible to maintain a defense's efficacy for some time, though it is unlikely to do so forever. In other cases, depending in large part on the specific way the opponent has found to defeat the technology, incremental changes may provide little benefit. For example, if an adversary has found a way to avoid the functioning of the technology entirely (one of the four strategies our work identified that were highlighted in my testimony), incremental change is unlikely to be enough. The importance of both short-term and long-term research projects is therefore a part of the "portfolio approach" to developing defenses our work suggested, where it is longer-term work that may be the source of the "fall back" defensive options if today's technologies are breached. Focusing disproportionately on shorter-term efforts risks creating a defense that cannot respond to future changes in the threat.

While it is easy to say that both short- and long-term focused work are needed, the resources available for supporting research and development are not infinite and resource constraints must limit the number and scale of activities that can be pursued simultaneously. As a result, in thinking about portfolios of defenses we are not suggesting that multiple "full scale" technology programs be pursued at once. Instead, what is needed is portfolios of smaller scale research, pilot, and technology evaluation efforts that maintain a group of options at differing levels of maturity that be then called on—and scaled up—if and when they are needed.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Jeff Self, Division Chief, U.S. Border Patrol

Questions submitted by Chairman David Wu

All Threats

Q1. You say in your testimony that Border Patrol has an "'all threats' strategy with anti-terrorism as our main priority." In a conversation with a CBP officer at a major port, our staff learned that on-the-ground officers estimate that drug interdictions have decreased by approximately 90 percent since CBP's focus shifted to terrorism. In your opinion, is that estimate accurate? If so, how is CBP working with DHS S&T to identify promising technologies to improve the rate of drug interdictions?

A1. The Border Patrol, along with CBP, was an active partner with ONDCP and DOJ in the development of the National Southwest Border Counternarcotics Strategy, which was publicly released in October 2007. The Border Patrol is working diligently to implement the numerous strategy objectives that relate to combating all border threats, including narcotics. In FY 2007, the Border Patrol increased agent staffing along with complementary tactical infrastructure and surveillance technology to make gains in the number of miles under operational control between the ports of entry. These increases have contributed to the decrease in the number of arrests of aliens entering the United States illegally and the increase in the amount of marijuana and cocaine seizures nationwide. Border Patrol marijuana seizures (1,859,299 pounds) increased 36 percent; over 99 percent of that amount was seized on the southern border with Mexico. Border Patrol cocaine seizures (14,242 pounds) increased 11 percent; over 89 percent was seized on the southern border with Mexico, just over nine percent in the coastal border sectors and less than two percent along the northern border with Canada.

CBP Border Patrol's area of responsibility (AOR) is focused between the official ports of entry, while CBP Office of Field Operations concentrates at the port of entry. The Border Patrol is unfamiliar with the CBP officer assertion regarding the reduction of drug interdiction. That being said, the U.S. Border Patrol is the Department's first line of defense in interdicting terrorists, terrorist weapons, including potential weapons of mass destruction—from entering the United States between the ports of entry. This complements the Border Patrol's traditional missions of interdicting illegal aliens and drugs and those who attempt to smuggle them across our borders between the ports of entry.

To carry out its mission, Border Patrol has a clear strategic goal: to establish and maintain operational control of the border of the United States. All of our efforts are focused on this goal. The Border Patrol's strategy consists of five main objectives:

- Establish substantial probability of apprehending terrorists and their weapons as they attempt to enter illegally between the ports of entry;
- Deter illegal entries through improved enforcement;
- Detect, apprehend, and deter smugglers of humans, drugs, and other contraband;
- Leverage "Smart Border" technology to multiply the effect of enforcement personnel; and
- Reduce crime in border communities and consequently improve quality of life and economic vitality of targeted areas.

Reports/Recommendations

Q2. Has the Homeland Security Science and Technology Advisory Committee or Homeland Security Institute prepared any reports or recommendations for U.S. Customs and Border Protection directly? If so, how did CBP use these recommendations?

A2. CBP has utilized the Homeland Security Institute (HSI) to conduct several studies. The first study was an analysis of CBP's apprehensions at the border, and the second was an operational assessment. Both of these studies, the outcomes and recommendations that followed, were intended to help CBP assess whether progress is being made in our border security mission. In short, HSI substantiated in their report that there has been a cumulative deterrent impact resulting from our regular operations and special initiatives such as Jump Start, Streamline, end of catch and

release, and interior repatriation. CBP also utilized HSI to help determine the initial staffing requirements for the Secure Border Initiative (SBI) Program Executive Office (PEO), including the resources required to manage the SBInet procurement.

Questions submitted by Representative Ralph M. Hall

Tunnels

Q1. What risk do tunnels pose to our border security?

A1. As the Border Patrol increases and expands its efforts along the border, there will always be methods that smugglers employ to try to penetrate and thwart our efforts. Cross-border tunnels have become one way of countering our success above ground. The success of the Border Patrol's mission above ground coincides with an increase in the amount of cross-border tunnel activity that has been found. It is more difficult and time consuming for smugglers to dig tunnels underground then to cross the border illegally above ground.

Cross-border tunnels pose a threat to the Nation's border security. While those tunnels discovered thus far have primarily served as a way to smuggle drugs, clandestine tunnels could be used for illegal alien entry or to smuggle of weapons of mass destruction (WMD) or potential terrorists into the United States.

The Border Patrol conducts below-ground sonar inspections in an attempt to find tunneling activity along the border, participates in multi-agency Tunnel Task Forces, and shares intelligence with partner agencies regarding this threat. The DHS Science and Technology (S&T) Directorate has an ongoing program which is looking for breakthrough technologies to improve our ability to detect cross-border tunnels/tunneling activity. The goal is to develop a technology, or a combination of technologies that Border Patrol officers and other enforcement agencies can use to monitor the border for tunnel construction.

As we gain effective control of the border, we expect to see smuggling organizations try other tactics, and we will adapt our efforts in order to shut those tactics down as well.

Red Tape

Q2. What red tape must Customs and Border Protection or S&T overcome in order to use UAVs routinely? How has the Unmanned Aircraft System (UAS) program stacked up against helicopters and airplanes in effectiveness and cost as a tool for the Border Patrol?

A2. U.S. Customs and Border Protection (CBP) continues to work closely with the Federal Aviation Administration (FAA) and the Department of Defense on issues affecting the use of unmanned aircraft in the national air space. To date, the FAA has been very cooperative in meeting CBP's air space access requirements. Through the Office of CBP Air and Marine (A&M), the Agency's plans for expanded use of unmanned aircraft across all of the Nation's borders are being addressed with the FAA. In FY 2008, CBP A&M intends to conduct a maritime demonstration of UAS capabilities in conjunction with the U.S. Coast Guard, and to introduce a UAS to the northern border area of responsibility.

The Predator B UAS provides CBP with a remotely piloted asset that allows for persistent, broad area surveillance with proactive responses that is driven by uncued, cued, and intelligence based missions. With a maximum range of 3,000 miles and the potential for 30 hours of on-station time, no other system in the CBP Air and Marine fleet provides the same capabilities as the Predator B. Instead of duplicating or replacing the capabilities of existing CBP assets, CBP A&M exploits the unique capabilities of the UAS to greatly enhance CBP's border security operations. The UAS will allow CBP A&M to support other DHS entities, including the U.S. Coast Guard, the Federal Emergency Management Agency (FEMA), and U.S. Immigration and Customs Enforcement (ICE). The FY 2008 Appropriation requires CBP to submit a cost effectiveness report to Congress. Once that report is submitted to the committees on appropriations, CBP will share that cost effectiveness information with the Committee.

FAA Restrictions

Q3. Currently the FAA requires that licensed pilots operate all aircraft in the National Airspace. The FAA does not allow fully autonomous aircraft to fly without special authorization. Would you expect a large increase in use of UAVs by the Border Patrol if these restrictions were lifted? Finally, has the Border Patrol

gained benefit from early trials of remotely-piloted UAVs and would you consider participating in similar trials for autonomous drones?

A3. CBP A&M does not expect a large increase in the use of unmanned aircraft systems for homeland security if the FAA lifted their restrictions on pilot qualifications and system capabilities. The use of instrument-rated pilots for operations in the national air space is a safety of flight issue and CBP would retain the requirement even if the FAA lifted their restrictions. UAS operations across the southwest border have proven highly effective. In just over 1,500 hours of flight operations, CBP UASs have been credited with over 4,000 apprehensions and the seizure of about 15,000 lbs of illegal drugs. The Predator B UAS has the capabilities to meet all current CBP mission requirements. Should new requirements emerge that the Predator B could not accommodate, CBP A&M would investigate the use of other aviation assets to meet the new mission need.

Questions submitted by Representative Adrian Smith

Fences

Q1. In your experience, where there are fences or physical barriers, are they singularly effective at preventing aliens from crossing the border illegally?

A1. Border infrastructure, in this case fences and physical barriers, is effective in certain areas. However, as experience and common sense suggests, fencing by itself cannot prevent all aliens from crossing the border illegally. There are stretches of fencing or barriers that are complemented by a presence of agents and technology to support the infrastructure, making the fencing and barriers operationally successful by preventing aliens from the crossing the border illegally. Technology allows the Border Patrol to identify and track illegal activity. Fencing helps deter illegal crossings and gives Border Patrol agents time they need to respond to illegal cross border activity. Fencing and barriers work hand in hand with manpower and technology to establish deterrence and increase the certainty of apprehension.

UAS

Q2. As you stated in your testimony, the Unmanned Aircraft System (UAS) has assisted immensely in arrests and seizure of illegal drugs. In your opinion, are these types on technologies more capable and effective at preventing illegal entry into our country than physical barriers?

A2. CBP is building a border security system comprised of many components, and each component complements one or more of the others. UASs provide intelligence-gathering and surveillance capabilities as well as direct support to ground and maritime interdiction operations. But the UAS cannot meet all Agency border security requirements. In addition to Border Patrol agents on the ground, physical barriers and sensors are required to cover the vast areas threatened by illegal activities. Threat information must be processed and returned to the field as actionable intelligence. Only though an integrated network of ground systems, air and marine systems, sensors, communications, intelligence, and people can CBP accomplish its homeland security mission.

Documents

Q3. How often do Border Patrol Agents come across fraudulent documents? What types of documents are most often tampered with? And how many documents must Border Patrol agents become familiar with?

A3. There have been fewer than 100 reported fraudulent documents encountered throughout the Border Patrol annually in the last five years.

For encounters with tampered documents, agents generally come across the older plastic covered I–551, Lawfully Admitted Permanent Resident (LAPR) card and I–94, Arrival/Departure Record. The older I–551 LAPR card was manipulated by photo substitutions and modifying the type within the card. The older I–551 LAPR card has been replaced with an updated holographic magnetic striped machine readable card with additional security features. The I–94 is a paper document that has computer type, ink stamping, an embossed seal and an attached photo. The I–94 is sometimes manipulated by photo substitutions and modifying the type and stamps.

Agents must become familiar with immigration documents and other local governmental issued documents. Examples of immigration documents are the I–551 LAPR

card, I–586 Border Crosser Card (BCC), I–94 and other foreign issued travel documents such as passports and visas. Other non immigration issued documents that Border Patrol Agents need to be familiar with are birth and marriage certificates, Social Security Cards and driver's licenses.

Appendix 2:

Additional Material for the Record

I

110TH CONGRESS
1ST SESSION

H. R. 3916

To provide for the next generation of border and maritime security technologies.

IN THE HOUSE OF REPRESENTATIVES

OCTOBER 22, 2007

Mr. HALL of Texas (for himself, Mr. BARTLETT of Maryland, Mr. BILBRAY, Mr. BROUN of Georgia, Mr. BURGESS, Mr. CONAWAY, Mr. FEENEY, Mr. GINGREY, Mr. GORDON of Tennessee, Mr. INGLIS of South Carolina, Mr. SAM JOHNSON of Texas, Mr. MCCAUL of Texas, Mrs. MYRICK, Mr. NEUGEBAUER, Mr. SENSENBRENNER, Mr. SESSIONS, Mr. SMITH of Nebraska, Mr. WU, Mrs. BIGGERT, and Mr. LAMPSON) introduced the following bill; which was referred to the Committee on Homeland Security, and in addition to the Committee on Science and Technology, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

To provide for the next generation of border and maritime security technologies.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

SECTION 1. ENSURING RESEARCH ACTIVITIES OF THE DEPARTMENT OF HOMELAND SECURITY INCLUDE APPROPRIATE CONCEPTS OF OPERATION.

The Under Secretary for Science and Technology of the Department of Homeland Security (in this Act referred to as the "Under Secretary") shall ensure that any Federal Government interagency or intra-agency agreement to develop and transition new technology explicitly characterizes the requirements, expected use, and concept of operations for that technology, including—

(1) the manpower needed to effectively operate the technology;

(2) the expected training requirements; and

(3) the expected operations and maintenance costs.

SEC. 2. REAUTHORIZATION OF HOMELAND SECURITY SCIENCE AND TECHNOLOGY ADVISORY COMMITTEE.

Section 311(j) of the Homeland Security Act of 2002 (6 U.S.C. 191(j)) is amended by striking "on December 31, 2008" and inserting "on December 31, 2012".

SEC. 3. REPORT ON BASIC RESEARCH NEEDS FOR BORDER/MARITIME SECURITY.

Not later than 3 months after the date of enactment of this Act, the Under Secretary shall enter into an ar-

1 rangement with the National Research Council for an as-
2 sessment of the basic science research needs in the border
3 and maritime security domain. The assessment shall in-
4 clude consideration of—
5 (1) detection, tracking, and identification tech-
6 nologies;
7 (2) personal protective equipment;
8 (3) anticounterfeit technologies; and
9 (4) advanced screening technologies at ports of
10 entry.

11 **SEC. 4. INCORPORATING UNMANNED AERIAL VEHICLES**
12 **INTO BORDER/MARITIME AIRSPACE.**

13 (a) RESEARCH AND DEVELOPMENT.—The Secretary
14 of Homeland Security and the Director of the Joint Plan-
15 ning and Development Office shall research and develop
16 technologies to permit routine operation of unmanned aer-
17 ial vehicles within the national airspace for border and
18 maritime security missions without any degradation of ex-
19 isting levels of safety for all national airspace system
20 users.

21 (b) PILOT PROJECTS.—The Secretary shall coordi-
22 nate with the Administrator of the Federal Aviation Ad-
23 ministration to enter into pilot projects in sparsely popu-
24 lated, low-density Class G air traffic airspace to conduct
25 experiments and collect data in order to accelerate the safe

integration of unmanned aircraft systems into the national airspace system.

SEC. 5. ESTABLISHING A RESEARCH PROGRAM IN TUNNEL DETECTION.

(a) RESEARCH AND DEVELOPMENT.—The Under Secretary shall research and develop technologies to permit detection of near surface voids, such as tunnels, with an emphasis on technologies with real time capability.

(b) COORDINATION.—The Secretary of Homeland Security shall coordinate with other appropriate Federal agencies, including the Department of Defense, and ensure the integration of activities under subsection (a) with relevant efforts of such other agencies and the Department of Homeland Security's Centers of Excellence Program.

SEC. 6. RESEARCH IN ANTICOUNTERFEIT TECHNOLOGIES.

(a) ESTABLISHMENT OF PROGRAM.—The Under Secretary and the Director of the National Institute of Standards and Technology shall establish a joint research and development program on anticounterfeit technologies and standards. The program may include development of counterfeit-resistant documentation, counterfeit-resistant devices, document validation technologies, and document identification standards.

1 (b) COORDINATION.—In carrying out the program in
2 subsection (a), the Under Secretary or his designee shall
3 coordinate with other Federal agencies engaged in similar
4 activities, including Immigration and Customs Enforce-
5 ment, the Department of State, the Department of De-
6 fense, and the Department of Justice.

7 (c) REPORT TO CONGRESS.—Not later than 12
8 months after the date of enactment of this Act, the Under
9 Secretary and the Director of the National Institute of
10 Standards and Technology shall provide to the Committee
11 on Homeland Security and the Committee on Science and
12 Technology of the House of Representatives, and the Com-
13 mittee on Homeland Security and Government Affairs of
14 the Senate, a report detailing the actions taken by the
15 Under Secretary and the Director under this section.

○