AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

TECHNOLOGY NEEDED TO SECURE AMERICA'S BORDER

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY
&
SUBCOMMITTEE ON OVERSIGHT

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

JULY 31, 2014

Serial No. 113–90

Printed for the use of the Committee on Science, Space, and Technology

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

U.S. GOVERNMENT PUBLISHING OFFICE
89–419PDF WASHINGTON : 2015

For sale by the Superintendent of Documents, U.S. Government Publishing 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, SPACE, AND TECHNOLOGY

HON. LAMAR S. SMITH, Texas, *Chair*

DANA ROHRABACHER, California
RALPH M. HALL, Texas
F. JAMES SENSENBRENNER, JR., Wisconsin
FRANK D. LUCAS, Oklahoma
RANDY NEUGEBAUER, Texas
MICHAEL T. McCAUL, Texas
PAUL C. BROUN, Georgia
STEVEN M. PALAZZO, Mississippi
MO BROOKS, Alabama
RANDY HULTGREN, Illinois
LARRY BUCSHON, Indiana
STEVE STOCKMAN, Texas
BILL POSEY, Florida
CYNTHIA LUMMIS, Wyoming
DAVID SCHWEIKERT, Arizona
THOMAS MASSIE, Kentucky
KEVIN CRAMER, North Dakota
JIM BRIDENSTINE, Oklahoma
RANDY WEBER, Texas
CHRIS COLLINS, New York
BILL JOHNSON, Ohio

EDDIE BERNICE JOHNSON, Texas
ZOE LOFGREN, California
DANIEL LIPINSKI, Illinois
DONNA F. EDWARDS, Maryland
FREDERICA S. WILSON, Florida
SUZANNE BONAMICI, Oregon
ERIC SWALWELL, California
DAN MAFFEI, New York
ALAN GRAYSON, Florida
JOSEPH KENNEDY III, Massachusetts
SCOTT PETERS, California
DEREK KILMER, Washington
AMI BERA, California
ELIZABETH ESTY, Connecticut
MARC VEASEY, Texas
JULIA BROWNLEY, California
ROBIN KELLY, Illinois
KATHERINE CLARK, Massachusetts

SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

HON. LARRY BUCSHON, Indiana, *Chair*

STEVEN M. PALAZZO, Mississippi
MO BROOKS, Alabama
RANDY HULTGREN, Illinois
STEVE STOCKMAN, Texas
CYNTHIA LUMMIS, Wyoming
DAVID SCHWEIKERT, Arizona
THOMAS MASSIE, Kentucky
JIM BRIDENSTINE, Oklahoma
CHRIS COLLINS, New York
BILL JOHNSON, Ohio
LAMAR S. SMITH, Texas

DANIEL LIPINSKI, Illinois
FEDERICA WILSON, Florida
ZOE LOFGREN, California
SCOTT PETERS, California
AMI BERA, California
DEREK KILMER, Washington
ELIZABETH ESTY, Connecticut
ROBIN KELLY, Illinois
EDDIE BERNICE JOHNSON, Texas

SUBCOMMITTEE ON OVERSIGHT

HON. PAUL C. BROUN, Georgia, *Chair*

F. JAMES SENSENBRENNER, JR., Wisconsin
BILL POSEY, Florida
KEVIN CRAMER, North Dakota
BILL JOHNSON, Ohio
LAMAR S. SMITH, Texas

DAN MAFFEI, New York
ERIC SWALWELL, California
SCOTT PETERS, California
EDDIE BERNICE JOHNSON, Texas

CONTENTS

July 31, 2014

	Page
Witness List	2
Hearing Charter	3

Opening Statements

Statement by Representative Larry Bucshon, Chairman, Subcommittee on Research and Technology, Committee on Science, Space, and Technology, U.S. House of Representatives	7
Written Statement	7
Statement by Representative Daniel Lipinski, Ranking Minority Member, Subcommittee on Research and Technology, Committee on Science, Space, and Technology, U.S. House of Representatives	8
Written Statement	9
Statement by Representative Paul Broun, Chairman, Subcommittee on Oversight, Committee on Science, Space, and Technology, U.S. House of Representatives	11
Written Statement	12
Statement by Representative Dan Maffei, Ranking Minority Member, Subcommittee on Research and Technology, Committee on Science, Space, and Technology, U.S. House of Representatives	12
Written Statement	13
Statement by Representative Lamar S. Smith, Chairman, Committee on Science, Space, and Technology, U.S. House of Representatives	14
Written Statement	15

Witnesses:

Dr. K. Jack Riley, Vice President, RAND National Security Research Division; Director, RAND National Defense Research Institute	
Oral Statement	16
Written Statement	18
Mr. David C. Maurer, Director, Homeland Security and Justice, U.S. Government Accountability Office	
Oral Statement	29
Written Statement	31
Dr. Joseph D. Eyerman, Director, Health Security Program, RTI International; Director for Research and Management, Institute for Homeland Security Solutions, Duke University	
Oral Statement	49
Written Statement	51
Discussion	57

Appendix I: Answers to Post-Hearing Questions

Dr. K. Jack Riley, Vice President, RAND National Security Research Division; Director, RAND National Defense Research Institute	68
Mr. David C. Maurer, Director, Homeland Security and Justice, U.S. Government Accountability Office	71

Page

Appendix II: Additional Material for the Record

Prepared statement by Representative Eddie Bernice Johnson, Ranking Member, Committee on Science, Space, and Technology, U.S. House of Representatives 82

Supporting information requested by Representative Lamar S. Smith, Chairman, Committee on Science, Space, and Technology, U.S. House of Representatives 84

TECHNOLOGY NEEDED TO SECURE AMERICA'S BORDER

THURSDAY, JULY 31, 2014

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY AND
SUBCOMMITTEE ON OVERSIGHT,
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, D.C.

The Subcommittees met, pursuant to call, at 10:07 a.m., in Room 2318 of the Rayburn House Office Building, Hon. Larry Bucshon [Chairman of the Subcommittee on Research and Technology] presiding.

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6371
www.science.house.gov

Subcommittee on Research and Technology
and
Subcommittee on Oversight

Technology Needed to Secure America's Border

Thursday, July 31, 2014
10:00 a.m. to 12:00 p.m.
2318 Rayburn House Office Building

Witnesses

***Dr. K. Jack Riley**, Vice President, RAND National Security Research Division; Director, RAND National Defense Research Institute*

***Mr. David C. Maurer**, Director, Homeland Security and Justice, U.S. Government Accountability Office*

***Dr. Joseph D. Eyerman**, Director, Health Security Program, RTI International; Director for Research and Management, Institute for Homeland Security Solutions, Duke University*

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY
SUBCOMMITTEE ON OVERSIGHT

HEARING CHARTER

Technology Needed to Secure America's Border

Thursday, July 31, 2014
10:00 a.m. – 12:00 p.m.
2318 Rayburn House Office Building

Purpose

On Thursday, July 31, 2014, the Subcommittee on Research and Technology and the Subcommittee on Oversight of the Committee on Science, Space, and Technology will hold a joint hearing to receive testimony from witnesses outside the Science and Technology (S&T) Directorate of the Department of Homeland Security (DHS) on the technologies needed to better secure our nation's borders. This hearing will inform the Committee on potential issues for discussion during a later hearing with the DHS Undersecretary of Science and Technology planned for September and subsequent legislation re-authorizing research and technology development projects within the S&T Directorate.

Witnesses

- **Dr. K. Jack Riley**, Vice President, RAND National Security Research Division; Director, RAND National Defense Research Institute
- **Mr. David C. Maurer**, Director, Homeland Security and Justice, U.S. Government Accountability Office
- **Dr. Joseph D. Eyerman**, Director, Health Security Program, RTI International; Director for Research and Management, Institute for Homeland Security Solutions, Duke University

Background

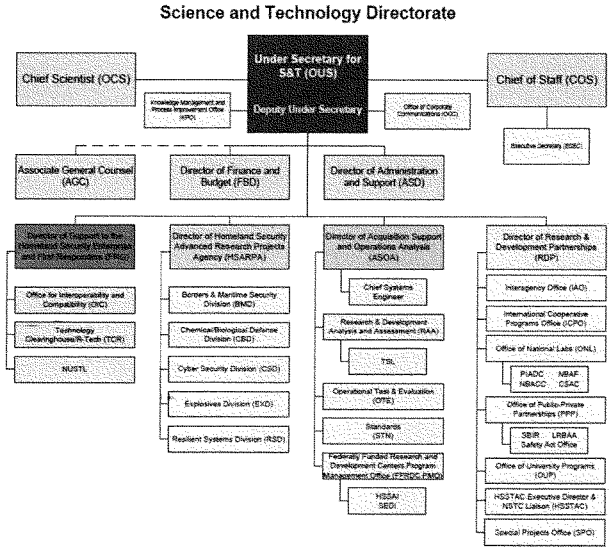
U.S. Customs and Border Protection (CBP) "welcomes nearly 1 million visitors, screens more than 67,000 cargo containers, arrests more than 1,100 individuals and seizes nearly 6 tons of illicit drugs" on a typical day.[1] CBP is also responsible for monitoring between legal entry points along the Northern and Southern borders and intercepting individuals attempting to cross the border. The Northern border of the United States and Canada is over 5,000 miles long. The Southwest border of the United States and Mexico is nearly 2,000 miles long.

[1] DHS U.S. Customs and Border Protection, available at: http://www.cbp.gov/about.

Surveillance technologies act as force multipliers for border patrol agents to augment "boots on the ground" with persistent observations from ground-based and airborne platforms. Many off-the-shelf surveillance technologies that are used at government and commercial facilities today are still not feasible to operationally deploy along the Southwest border. The DHS S&T Directorate has primary responsibility for bringing new technologies to full readiness, including technologies needed to better secure out nation's border, with support from other agencies, including the Department of Defense and National Institute of Standards and Technology.

Department of Homeland Security Science and Technology Directorate

In 2002, Title III of the Homeland Security Act (PL 107-296) established the role of Undersecretary for Science and Technology, the Directorate for S&T, and the Homeland Security Advanced Research Projects Agency (HSARPA) within DHS. The S&T Directorate is responsible for managing and carrying out science and technology research on behalf of federal homeland security needs and coordinating this research with other federal research entities.[2] The Committee on Science, Space, and Technology shares oversight of the S&T Directorate with the Homeland Security Committee. The current organization of the directorate has been in place since 2010:[3]



[2] Title III of P.L. 107-296, available at: http://www.gpo.gov/fdsys/pkg/PLAW-107publ296/pdf/PLAW-107publ296.pdf.
[3] DHS Science and Technology Directorate, available at: https://www.dhs.gov/sites/default/files/publications/ST%20Org%20Chart-12-2012_0.pdf.

The S&T Directorate is currently funded at approximately $1.2 billion in FY2014, and the Administration has requested $1.07 billion for FY 2015.

Science and Technology Directorate (DHS S&T) Spending
(dollars in millions)

Account	FY13* Enacted	FY14** Enacted	FY15 Request	FY15 Request versus FY14 Enacted	
				$	%
Science and Technology Directorate					
Acquisition and Operations Support	*46.0*	*41.7*	*41.7*	-	-
Laboratory Facilities	*158.1*	*547.8*	*435.2*	*(112.6)*	*(21)*
Research, Development, and Innovation	*425.3*	*462.0*	*433.8*	*(28.2)*	*(6)*
University Programs	*38.3*	*39.7*	*31.0*	*(8.7)*	*(22)*
Management and Administration	*126.5*	*129.0*	*130.1*	*1.1*	*.85*
Totals:	**797.1**	**1,220.1**	**1,071.8**	**(148.3)**	**(12)**

*FY 13 totals include emergency/supplemental funding and rescission.
**FY 14 totals include a rescission.

***Source**: FY 2015 Budget in Brief – Homeland Security*

Government Accountability Office (GAO) Reports

The Government Accountability Office has reviewed the work and produced reports related to DHS S&T as well as the technology deployment delays on the border fence for many years. In September 2012, GAO released a report titled, *Department of Homeland Security Oversight and Coordination of Research and Development Should Be Strengthened.*[4] GAO found that DHS does not know how much its components spend on research and development (R&D) and does not have policies and guidance for defining R&D and overseeing R&D resources across the Department. According to DHS, the S&T Directorate, the Domestic Nuclear Detection Office (DNDO), and U. S. Coast Guard are the only components that conduct R&D. However, GAO identified an additional $255 million in R&D being conducted by other DHS components. Some of this R&D was found to be similar or duplicative of other work already on-going. As a result, GAO recommended that DHS develop policies and guidance for defining, reporting, and coordinating R&D activities across the Department. GAO also recommended that DHS establish a better mechanism to track R&D projects.[5]

[4] GAO Report, "Department of Homeland Security Oversight and Coordination of Research and Development Should Be Strengthened," September 2012, available at: http://www.gao.gov/assets/650/648152.pdf.
[5] Ibid.

In a September 2013 report titled, *Department of Homeland Security Opportunities Exist to Better Evaluate and Coordinate Border and Maritime Research and Development,*[6] GAO found that DHS border and maritime R&D components reported producing 97 R&D deliverables between 2010 and 2012, at an estimated cost of $177 million. Customers expressed mixed views on the impact of these wide-ranging R&D products.[7]

According to the 2013 report, while DHS is working to develop policies to define and coordinate R&D, additional actions could strengthen internal and external coordination of border and maritime R&D. Work still needs to be done at the agency level to make sure border and maritime R&D efforts are mutually reinforcing and being directed towards the highest priority needs. As a result, GAO recommended that S&T establish "timeframes and milestones for collecting and evaluating feedback from its customers to determine the usefulness and impact of its R&D efforts."[8] GAO also recommended that S&T ensure potential challenges with data reliability, accessibility, and availability are reviewed and understood before approving Centers of Excellence R&D projects.[9]

Additional Reading

Beyond these two reports focused on the S&T Directorate, GAO has published several others on the operational and technology deployment challenges to better secure our national borders. The following reports are informative to the Committee:

- Border Security: DHS's Progress and Challenges in Securing U.S. borders. GAO-13-414T. Washington, D.C.: March 14, 2013. http://www.gao.gov/assets/660/653037.pdf

- Border Security: Opportunities Exist to Ensure More Effective Use of DHS's Air and Marine Assets. GAO-12-518. Washington, D.C.: March 30, 2012. http://www.gao.gov/assets/590/589797.pdf

- Arizona Border Surveillance Technology: More Information on Plans and Costs Is Needed before Proceeding. GAO-12-22. Washington, D.C.: November 4, 2011. http://www.gao.gov/assets/590/586102.pdf

- Secure Border Initiative: DHS Has Faced Challenges Deploying Technology and Fencing Along the Southwest Border. GAO-10-651T. Washington, D.C.: May 4, 2010. http://www.gao.gov/assets/90/82411.pdf

- Secure Border Initiative: Technology Deployment Delays Persist and the Impact of Border Fencing Has Not Been Assessed. GAO-09-896. Washington, D.C.: September 9, 2009. http://www.gao.gov/assets/300/294982.pdf

---

[6] GAO Report, "Department of Homeland Security Opportunities Exist to Better Evaluate and Coordinate Border and Maritime Research and Development," September 2013, available at: http://www.gao.gov/assets/660/658112.pdf.
[7] Ibid.
[8] Ibid.
[9] Ibid.

Chairman BUCSHON. Good morning. This joint hearing of the Subcommittee on Research and Technology and the Subcommittee on Oversight will come to order.

Good morning, and welcome to today's joint hearing titled "Technology Needed to Secure America's Border."

In front of you are packets containing the written testimony, biographies and Truth in Testimony disclosures for today's witnesses.

Before we get started, since this is a joint hearing involving two Subcommittees, I want to explain how we will operate procedurally so that all Members understand how the question-and-answer period will be handled. We will recognize those Members present at the gavel in order of seniority on the full Committee and those coming in after the gavel will be recognized in order of arrival. I recognize myself now for five minutes for an opening statement.

Twelve years ago, the Homeland Security Act established the Directorate for Science and Technology within the Department of Homeland Security. The S&T Directorate manages and carries out science and technology research for our federal homeland security needs. The Directorate is also responsible for coordinating this research with other federal research entities. The Committee on Science, Space, and Technology shares oversight of the S&T Directorate with the Homeland Security Committee.

Since this spring, this Subcommittee had been planning a joint hearing with our counterparts in the Homeland Security Committee to hear from the Department of Homeland Security S&T Directorate, so this has been a long-planned hearing. It is just that today is the day that it would work for us to do this. Unfortunately, the Department of Homeland Security could not work that into their schedule but there will be another hearing in September that will complete this hearing.

Unfortunately, we could not make the calendars come together, like I said, and I am looking forward to the Department of Homeland Security testifying in September.

The DHS S&T Directorate is responsible for developing new technologies from basic research to development for use, including technologies that can help to secure our Nation's border. From unmanned aerial vehicles, to tunnel detection, from anti-counterfeit standards to biometrics, there are existing and promising new technologies that can act as force multipliers for Border Patrol agents and the Coast Guard to augment their day-to-day work on border security related issues.

We will hear this morning from the Government Accountability Office, which has issued a series of reports about DHS technology research and development, and from two private-sector experts, each of whom can contribute on a different aspect of border security technology. I look forward to hearing from all of our witnesses.

[The prepared statement of Mr. Bucshon follows:]

PREPARED STATEMENT OF THE SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY
CHAIRMAN LARRY BUCSHON

Twelve years ago, the Homeland Security Act (PL 107-296) established the Directorate for Science and Technology (S&T Directorate) within the Department of Homeland Security (DHS).

The S&T Directorate manages and carries out science and technology research for our federal homeland security needs. The Directorate is also responsible for coordinating this research with other federal research entities. The Committee on Science, Space, and Technology shares oversight of the S&T Directorate with the Homeland Security Committee.

Since this spring, this Subcommittee had been planning a joint hearing with our counterparts in the Homeland Security Committee to hear from the Department of Homeland Security S&T Directorate. Unfortunately, we could not make our Subcommittee's calendars meet this month so we will use this hearing to inform a joint hearing in September. At that hearing, we will focus on testimony and discussion with the head of DHS S&T.

The DHS S&T Directorate is responsible developing new technologies from basic research to development for use, including technologies that can help to secure our nation's border. From unmanned aerial vehicles, to tunnel detection, from anti-counterfeit standards to biometrics, there are existing and promising new technologies that can act as force multipliers for border patrol agents and the Coast Guard to augment their day to day work on border security related issues.

We will hear this morning from the Government Accountability Office, which has issued a series of reports about DHS Technology research and development, and from two private sector experts, each of whom can contribute on a different aspect of border security technology. I look forward to hearing from all of our witnesses.

Chairman BUCSHON. I now recognize the Ranking Member, the gentleman from Illinois, Mr. Lipinski, for an opening statement.

Mr. LIPINSKI. Thank you, Mr. Chairman, for calling this hearing today, and thank you to our witnesses for providing valuable testimony on this issue.

Today we will hear about how the Department of Homeland Security can improve its research and development efforts on technology to secure America's borders. With growing turmoil around the world, the threats we face at our borders are more pressing than ever. These threats include terrorists and criminals entering our country, human trafficking, drug trafficking, and other dangerous materials and substances being smuggled into the United States. As has been said many times, those wishing America harm only need to get it right once. To keep America safe, we need to get it right every time. This daunting task falls largely on the shoulders of DHS.

As a member of both the Science, Space, and Technology Committee and the Transportation and Infrastructure Committee, I am especially concerned with border security as it relates to transportation. Last week I met with the Commissioner of U.S. Customs and Border Protection, Gil Kerlikowske, on their efforts to develop technologies such as the fingerprint scanners at O'Hare Airport in Chicago as part of CBP's Global Entry program.

Science and technology plays a critical role in addressing our homeland security challenge. However, the Department has been plagued with problems in its planning and management of research and development. The agency is young, having been only created 11 years ago. While I do not envy the task of stitching together several government programs and functions into a new agency, I remain concerned that several of the problems we saw in the agency's initial years remain today.

As GAO has previously stated, the Department cannot tell us how much they invest in R&D. There is a lack of effective communication between operational components and the Science and Technology Directorate. Furthermore, there is still no strategic plan in place to guide the Department's research and development activities.

It is important to understand the steps the agency goes through when identifying and solving a technological problem, whether for border security or another mission need. When agents in the field identify a technological challenge, how is this need passed along to the researchers developing the technology? The communication between the operational components of DHS and the researchers at the Science and Technology Directorate has to be improved.

Once a technology is developed, it must be thoroughly tested and evaluated to see that it not only functions as intended, but is adapted for the environment in which it will operate. Understanding how CBP agents or other customers in the field will use the technology and what additional improvements should be made is a key step in successfully deploying the technology. Without understanding the human elements in this process, I am concerned we could be investing significant federal resources in potentially unusable technology. I look forward to hearing from Dr. Eyerman about the importance of social science in the evaluation and deployment of new technologies at DHS.

Securing our borders is a difficult and complex problem. People and materials can enter by air, land, and sea. This requires our border security efforts to not only effectively communicate internally, but also coordinate with other federal agencies, as well as state and local governments. I hope our discussion today provides the Committee with recommendations to inform our oversight and legislative responsibilities for R&D at the Department of Homeland Security. And I look forward to hearing about how public- and private-sector innovation can help protect the American border.

Thank you Mr. Chairman. I yield back the balance of my time.

[The prepared statement of Mr. Lipinski follows:]

PREPARED STATEMENT OF THE SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY
RANKING MINORITY MEMBER DANIEL LIPINSKI

Thank you Mr. Chairman for calling this hearing today, and thank you to the witnesses for providing valuable testimony on this issue.

Today we will hear about how the Department of Homeland Security can improve its research and development efforts on technology to secure America's borders. With growing turmoil around the world, the threats we face at our borders are more pressing than ever. These threats include terrorists and criminals entering our country, human trafficking, drug trafficking, and other dangerous materials and substances being smuggled into the U.S. As has been said many times, those wishing America harm only need to get it right once—to keep America safe, we need to get it right every time. This daunting task falls largely on the shoulders of DHS. As a member of both the Science, Space, and Technology Committee and the Transportation and Infrastructure Committee, I am especially concerned with border security as it relates to transportation. Last week I met with the Commissioner of U.S. Customs and Border Protection, Gil Kerlikowske, on their efforts to develop technologies such as the fingerprint scanners at O'Hare Airport in Chicago as part of CBP's Global Entry program.

Science and technology plays a critical role in addressing our homeland security challenges. However, the Department has been plagued with problems in its planning and management of research and development. The agency is young, having only been created 11 years ago. While I do not envy the task of stitching together several government programs and functions into a new agency, I remain concerned that several of the problems we saw in the agency's initial yearsremain today.

As GAO has previously stated, the Department cannot tell us how much they invest in R&D. There is a lack of effective communication between operational components and the Science & Technology Directorate. Furthermore, there is still no strategic plan in place to guide the Department's research and development activities.

It is important to understand the steps the agency goes through when identifying and solving a technological problem, whether for border security or another mission need. When agents in the field identify a technological challenge, how is this need passed along to the researchers developing the technology? The communication between the operational components of DHS and the researchers at the Science & Technology Directorate must be improved.

Once a technology is developed it must be thoroughly tested and evaluated to see that it not only functions as intended, but is adapted for the environment in which it will operate. Understanding how CBP agents or other customers in the field will use the technology and what additional improvements should be made is a key step in successfully deploying the technology. Without understanding the human elements in this process, I am concerned we could be investing significant federal resources in potentially unusable technology. I look forward to hearing from Dr. Eyerman about the importance of social science in the evaluation and deployment of new technologies at DHS.

Securing our borders is a difficult and complex problem. People and materials can enter by air, land, and sea. This requires our border security efforts to not only effectively communicate internally, but also coordinate with other federal agencies, as well as state and local governments. I hope our discussion today provides the Committee with recommendations to inform our oversight and legislative responsibilities for R&D at the Department of Homeland Security. And I look forward to hearing about how public and private sector innovation can help protect the American border.

Thank you Mr. Chairman. I yield back the balance of my time.

Chairman BUCSHON. Thank you, Mr. Lipinski. The Chair now recognizes the Chairman of the Subcommittee on Oversight, the gentleman from Georgia, Dr. Broun, for his opening statement.

Chairman BROUN. Thank you, Dr. Bucshon, and I welcome all of you all here today as witnesses, and I am looking forward to hearing from all of you all about this very important issue.

Earlier this month, I traveled to the southern border of our country with the Homeland Security Committee. We held a field hearing in McAllen, Texas, on July 3rd where we discussed the recent surge of unaccompanied minors (UACs) crossing the border. I was astounded to learn that the number of children illegally entering the United States from Central America has grown from approximately 5,000 of them a year to an estimated 57,000 so far this year, and they are projecting up to 90,000 in this fiscal year. An influx of this extent raises questions about the security of our southern border. Currently, Border Patrol agents are inundated with processing unaccompanied minors and not fulfilling their primary mission to safeguard the border against terrorists entering the country under the radar as well as drugs and other things that are entering. It is a national security issue as far as I am concerned.

In order to protect the nearly 2,000-mile southwest border, patrol agents would benefit from advances in modern technology such as video monitors, sensors, radars, cameras, thermal-imaging devices, and drones. However, there are many flaws within the various DHS components that conduct technology research and development, which include problems in the management, coordination, and acquisition of items needed to help secure our American border.

A 2012 GAO report notes that, "The Department of Homeland Security does not know the total amount its components invest in research and development and does not have policies and guidance for defining R&D and overseeing R&D resources across the Department." Further, a 2013 GAO report cites examples where projects were delayed and cancelled due to an inability to obtain data from DHS. This is intolerable.

The DHS Science and Technology Directorate states on its own Web site that it is "the primary research and development arm of the Department of Homeland Security and manages science and technology research, from development through transition, for the Department's operational components and first responders to protect the homeland." How can this primary research and development arm not have any idea of the total amount of taxpayer money being invested on technology to detect, prevent, and mitigate threats to our Nation? This is not the prescription to protect our homeland.

As the Chairman of this Committee's Oversight Subcommittee, I value transparency and accountability. The S&T Directorate needs to lay out a clear and comprehensive plan to manage research and development activities and coordinate with other entities to ensure the deployment of effective state-of-the-art technology in a timely fashion. Absent a strategic technology roadmap, our citizens will remain vulnerable to threats stemming from our unsecure border.

Thank you, Dr. Bucshon, and thank you, Mr. Chairman, for holding this very important hearing, and I yield back the balance of my time.

[The prepared statement of Mr. Broun follows:]

PREPARED STATEMENT OF THE SUBCOMMITTEE ON OVERSIGHT
CHAIRMAN PAUL BROUN

Earlier this month, I traveled to the Southern border of our country with the Homeland Security Committee. We held a field hearing in McAllen, Texas, where we discussed the recent surge of unaccompanied minors crossing the border. I was astounded to learn that the number of children illegally entering the United States from Central America has grown from under 5,000 a year to an estimated 57,000 so far this year. An influx of this extent raises questions about the security of our Southern border. Currently, border patrol agents are inundated with processing unaccompanied minors and not fulfilling their primary mission to safeguard the border against terrorists entering the country under the radar.

In order to protect the nearly 2,000 mile Southwest border, patrol agents would benefit from advances in modern technology such as video monitors, sensors, radars, cameras, thermal-imaging devices, and drones. However, there are many flaws within the various DHS components that conduct technology research and development, which include problems in the management, coordination, and acquisition of items needed to help secure the American border.

A 2012 GAO report notes that, "The Department of Homeland Security does not know the total amount its components invest in research and development and does not have policies and guidance for defining R&D and overseeing R&D resources across the Department." Further, a 2013 GAO report cites examples where projects were delayed and cancelled due to an inability to obtain data from DHS.

This is intolerable. The DHS Science and Technology Directorate states on its own website that it is "the primary research and development arm of the Department of Homeland Security and manages science and technology research, from development through transition, for the Department's operational components and first responders to protect the homeland." How can this primary research and development arm not have any idea of the total amount of taxpayer money being invested on technology to detect, prevent, and mitigate threats to our nation? This is not the prescription to protect our homeland.

As the Chairman of this Committee's Oversight Subcommittee, I value transparency and accountability. The S&T Directorate needs to lay out a clear and comprehensive plan to manage research and development activities, and coordinate with other entities to ensure the deployment of effective state-of-the-art technology in a timely fashion. Absent a strategic technology roadmap, our citizens will remain vulnerable to the threats stemming from an unsecure border.

Thank you again, Chairman Bucshon, for holding this very important hearing, and I yield back the balance of my time.

Chairman BUCSHON. Thank you, Dr. Broun. The Chair now recognizes the Ranking Member of the Subcommittee on Oversight, Mr. Maffei of New York, for his opening statement.

Mr. MAFFEI. Thank you very much, Mr. Chairman, and thank you, Chairman Bucshon, for holding this hearing, and I want to thank Chairman Broun as well and Ranking Member Lipinski.

Our current system and approach to immigration is clearly not working. The challenges are complex and must be dealt with in a bipartisan way. The only way to fully address these challenges and make sure the crisis of unaccompanied children coming over the border is taken care of is to enact bipartisan comprehensive immigration reform. That is why I have cosponsored the bipartisan legislation that would, bolster security at our borders and uphold the immigration laws already on the books. The Senate has already passed this bipartisan immigration reform bill by a wide margin, and I do believe it is time for the House to act as well, at least to bring it up for a vote.

What is essential is that we strengthen our borders and enforce our laws. That is essential to any nation's sovereignty, to control its own borders. But I want to say that I agree with Mr. Broun, my friend, Mr. Broun from Georgia, that border security must be focused on keeping terrorists and weapons of mass destruction as well as illegal firearms and dangerous drugs entering the United States, again, the need for reform.

For the purposes of this hearing, I look forward to hearing witnesses' testimony on the research, development, and implementation of new technologies on America's border and potential new technologies that might be more effective. It is unfortunate that the Committee was unable to obtain witnesses from the Department of Homeland Security's Science and Technology Directorate or host a joint hearing with the House Homeland Security Committee, as there is much overlap in this area, and that would have been more helpful.

That said, I am very grateful to the Chairs for calling this hearing. It is extremely important. It is important in my district, which does have a border. It is a border with Canada, but I do want to also know what is going on in the northern border, and I know Dr. Maurer would probably share that interest since his family is from Wayne County, which is in my district and does have that water border with Canada.

Being able to accurately monitor the integrity of U.S. borders is essential to maintaining border and national security, which is essential to our sovereignty. I look forward to our witnesses helping us to better understand the science behind these issues, and evaluate how technology can augment and support the human resources that are ultimately responsible for maintaining our border security.

I yield back.

[The prepared statement of Mr. Maffei follows:]

PREPARED STATEMENT OF THE SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY
RANKING MINORITY MEMBER DAN MAFFEI

Thank you Chairman Broun and Chairman Buschon for holding this hearing today.

I believe we need to get serious and work to secure and strengthen our borders and enforce the laws already on the books. Our current system and approach to immigration is not working and we need comprehensive reform now, which is why I've cosponsored bipartisan legislation that would, bolster security at our borders and uphold the immigration laws already on the books. The Senate has already passed this bipartisan comprehensive immigration reform bill by a wide margin and it is time for the House to act as well. Border security is also about keeping terrorists and weapons of mass destruction from reaching our shores.

For the purposes of this hearing, I look forward to hearing witness testimony on the research, development, and implementation of new technologies on America's border. It is unfortunate that the Committee was unable to obtain witnesses from the Department of Homeland Security's Science & Technology (S&T) Directorate or host a joint hearing with the House Homeland Security Committee, as there is much overlap in this issue area.

My District shares a nautical border with Canada, and I would like to know learn more about what is being done to secure the Northern Border, in addition to the Southern Border.

Being able to accurately monitor the integrity of U.S. borders is essential to maintaining border and national security. I look forward to our witnesses helping us to better understand the science behind these issues, and evaluate how technology can augment and support our human resources that are ultimately responsible for maintaining U.S border security.

Chairman BUCSHON. Thank you. I now recognize the Chairman of the full Committee, the gentleman from Texas.

Chairman SMITH. Thank you, Mr. Chairman.

Now, we all are aware of the impact of illegal immigrant children who stream across our southern border. This is both a national security and a humanitarian crisis that we cannot allow to continue. A country that has lost control of its borders has lost control of its future.

The President has ignored, failed to enforce, undermined, and unilaterally changed current immigration laws. As a result, millions of young people have risked their lives to make the dangerous trip and come here illegally. Further, the Administration has yet to present a plan to secure our Nation's borders. As border agents are forced to turn increased attention to the surge of minors concentrated in certain areas along the border, it leaves much of the rest of the border unprotected.

Technology is a key component to securing our 2,000 mile Southern border. Customs and Border Protection and National Guard troops cannot be everywhere. Sensors deployed along the border can detect and track the "coyotes" who smuggle children as well as illegal drugs and firearms across the border. Sensors will help Border Patrol agents know where coyotes are so that they can intercept and stop them. And ground-penetrating radar can find buried tunnels that crisscross our border.

We need to get this technology in the hands of our immigration officers. Unfortunately, the Department of Homeland Security has a poor track record when it comes to developing and fielding sensors and tactical communications infrastructure along the southwest border.

The Government Accountability Office (GAO) finds the Department of Homeland Security's research and development efforts to be "fragmented and overlapping." The Department's Science and Technology Directorate will spend $1.2 billion this year on numerous projects, some related to border security, but many are not. As in previous years, the GAO found hundreds of millions of dollars being spent each year on duplicative R&D projects by other offices within the Department. Frankly, no one knows who is in charge of research and development, or what the goal is. The GAO reports that the Science and Technology Directorate lost touch with its end users about what technologies and R&D projects should be a priority.

Today's witnesses will testify on the need for the Department of Homeland Security to develop a plan to secure America's borders and how best to carry out that plan. Research and technology are key components to securing America's borders.

In September, we will hear from the Department of Homeland Security Undersecretary for Science and Technology, a position created by this Committee in founding the Department, in a joint hearing with the Homeland Security Committee. We are working with them on draft legislation to set priorities for the Science and Technology Directorate on how to secure America's borders. I look forward to working with my colleagues in the weeks ahead to turn this goal into a reality.

While there may be mixed feelings about the current situation on our southern border, we should all be able to agree that we can and we must secure America's borders with the help of technology.

Thank you, Mr. Chairman. Yield back.

[The prepared statement of Mr. Smith follows:]

PREPARED STATEMENT OF FULL COMMITTEE CHAIRMAN LAMAR S. SMITH

Thank you, Chairman Bucshon for holding this hearing. We all are aware of the impact of illegal immigrant children who stream across our Southern border. This is both a national security and a humanitarian crisis that we cannot allow to continue. A country that has lost control of its borders has lost control of its future.

The President has ignored, failed to enforce, undermined, and unilaterally changed current immigration laws. As a result, millions of young people have risked their lives to make the dangerous trip and come here illegally.

Further, the Administration has yet to present a plan to secure our nation's borders. As border agents are forced to turn increased attention to the surge of minors concentrated in certain areas along the border, it leaves much of the rest of the border unprotected.

Technology is a key component to securing our 2,000 mile Southern border. Customs and Border Protection and National Guard troops cannot be everywhere.

Sensors deployed along the border can detect and track the "coyotes" who smuggle children—as well as illegal drugs and firearms—across the border. Sensors will help Border Patrol agents know where coyotes are so that they can intercept and stop them. And ground-penetrating radar can find buried tunnels that crisscross our border.

We need to get this technology in the hands of our immigration officers. Unfortunately, the Department of Homeland Security has a poor track record when it comes to developing and fielding sensors and tactical communications infrastructure along the Southwest border.

The Government Accountability Office (GAO) finds the Department of Homeland Security's research and development (R&D) efforts to be "fragmented and overlapping."

The Department's Science and Technology Directorate will spend $1.2 billion this year on numerous projects, some related to border security, but many are not. As in previous years, the GAO found hundreds of millions of dollars being spent each year on duplicative R&D projects by other offices within the department.

Frankly, no one knows who's in charge of research and development, or what the goal is. The GAO reports that the Science and Technology Directorate lost touch with its end-users about what technologies and R&D projects should be a priority.

Today's witnesses will testify on the need for the Department of Homeland Security to develop a plan to secure America's borders and how best to carry out that plan. Research and technology are key components to securing America's borders.

In September, we will hear from the Department of Homeland Security Undersecretary for Science and Technology—a position created by this Committee in founding the department—in a joint hearing with the Homeland Security Committee.

We are working with them on draft legislation to set priorities for the Science and Technology Directorate on how to secure America's borders.I look forward to working with my colleagues in the weeks ahead to turn this goal into a reality. While there may be mixed feelings about the current situation on our Southern border, we should all be able to agree that we can—and we must—secure America's borders with the help of technology.

Chairman BUCSHON. Thank you, Chairman.

If there are Members who wish to submit additional opening statements, your statements will be added to the record at this point.

Chairman BUCSHON. At this point I would like to introduce our witnesses. Our first witness, Dr. Jack Riley, is Vice President of RAND's National Security Research Division and Director of the National Defense Research Institute. Dr. Riley received his bachelor's from the University of Michigan, his master's from Georgetown, and his Ph.D. from the RAND Graduate School.

Our second witness is Mr. David Maurer. He is a Director at the U.S. Government Accountability Office's Homeland Security and Justice Team. Mr. Maurer earned his bachelor's from Michigan State, the competition right next door, and his two master's degrees from the University of Michigan and National Defense University.

Our third witness is Dr. Joseph Eyerman. Dr. Eyerman is Co-Director of the Institute for Homeland Security Solutions, a senior research methodologist, and the Director of RTI International Center for Security, Safety and Defense. Dr. Eyerman received his bachelor's from Muskingum University, his two master's degrees from Florida State University and Miami University, and his Ph.D. from Florida State University. Welcome to all our witnesses.

As our witnesses should know, spoken testimony is limited to five minutes each after which Members of the Committee will have five minutes each to ask questions.

It is the practice of the Subcommittee on Oversight to receive testimony under oath. Does anyone have a problem with that? If not, please stand and raise your right hand. Do you solemnly swear to affirm to tell the whole truth and nothing but the truth, so help you God? Let the record reflect that all the witnesses—you may be seated. Let the record reflect that all the witnesses participating have taken the oath.

At this point I recognize Dr. Riley for five minutes to present his testimony.

TESTIMONY OF DR. K. JACK RILEY, VICE PRESIDENT, RAND NATIONAL SECURITY RESEARCH DIVISION; DIRECTOR, RAND NATIONAL DEFENSE RESEARCH INSTITUTE

Dr. RILEY. Thank you, Chairmen Bucshon and Broun and Ranking Members Lipinski and Maffei, for the opportunity to testify today about strategic planning and technology needs for air, land and sea border security.

Almost exactly eight years ago, I testified before two Homeland Security Subcommittees on this same topic, and at that time I said, and I quote, "We have woefully underinvested in developing, evaluating and refining a comprehensive and integrated border security strategy. We have invested in numerous border security programs and initiatives but the impacts and the costs and the cost-effectiveness of virtually all of these initiatives are poorly understood."

Unfortunately, nearly a decade later, the same concerns still largely apply. So let me turn to three points that I will make in this testimony.

First, we need to invest in measurement and data so that we have an empirical basis from which to have policy debates; second, we need to invest in more systematically understanding the cost-effectiveness of programs and policies; and third and finally, we need to systematically track and document how border control efforts affect the larger economy and society.

Let me start my first point by explaining why the data gaps are so worrisome. Effective border security begins with understanding why and how people and contraband cross the border. Different motivations may require different policies. Migration, for example, motivated by the desire for economic betterment may be best con-

trolled by a combination of border deterrence and labor-market enforcement. In contrast, smuggling of contraband may be best addressed by deterrence and technological detection.

In my written testimony, I detail some of the ways in which we can capture this kind of data. However, as far as I can tell, none of these estimation methods have been formally adopted nor do they receive continued support for development and refinement. They should, however, so that they can become the foundation for a border security scorecard.

I will turn now to my second point, why it is important to know about cost-effectiveness. Imagine that Secretary Johnson is presented with the opportunity to add 10,000 Border Patrol agents. Using the kind of data I just mentioned, he could not only assess the effectiveness of additional agents but give guidance on where and how to deploy them. We could also give guidance on what technologies might be good substitutes for or complements to the additional personnel. But equally importantly, we could say something about how migrants and smugglers would adapt to the presence of additional personnel. Indeed, with better data, we might be able to predict how behavior might adapt, and correspondingly modify our policies. At minimum, we would likely detect the changes in behavior earlier, which in turn would help improving future policymaking.

Third, a word about the broader economic and social implications of the border. Policies designed to improve control over the border can propagate widely throughout the economy and society. To give one example, after 9/11 we changed visa policies to make it more difficult for terrorists to travel to the United States. However, by making it more difficult, we deter not only terrorists but also an unknown number of legitimate travelers—foreign tourists, foreign students, qualified foreign workers, whose presence provide great benefits to our economy and the vibrancy of our culture. In short, border enforcement directly and indirectly touches on every aspect of the economy and our livelihoods, and we should be systemically tracking these effects so that we understand the full costs and the full benefits of border security programs.

At the beginning of this oral statement I mentioned I have three points. However, I want to add a fourth. Border security is one of the greatest analytic challenges of the post-9/11 generation. It is a topic that can and should attract the best and the brightest minds. But it remains frustratingly difficult to work on the topic both because of departmental restrictions on access to the data that are collected and also because of departmental restrictions on publishing and academic engagement. Good science demands public scrutiny and rigorous academic engagement. I urge this Committee and the Subcommittees to exercise its oversight role and help make this topic better grounded in science and more attractive to the best analysts and researchers.

Thank you for the opportunity to testify today, and I look forward to your questions.

[The prepared statement of Dr. Riley follows:]

Testimony

Strategic Planning for Border Security

K. Jack Riley

RAND Office of External Affairs

CT-415

July 2014

Testimony presented before the House Science, Space, and Technology Committee, Subcommittee on Research and Technology and Subcommittee on Oversight on July 31, 2014

This product is part of the RAND Corporation testimony series. RAND testimonies record 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. **RAND®** is a registered trademark.

Published 2014 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Email: order@rand.org

K. Jack Riley[1]
The RAND Corporation

Strategic Planning for Border Security[2]

Before the Committee on Science, Space, and Technology
Subcommittee on Research and Technology
Subcommittee on Oversight
United States House of Representatives

July 31, 2014

Thank you, Chairmen Buschon and Broun and Ranking Members Lipinski and Maffei, for the opportunity to testify today on the strategic planning and technology dimensions of land, air and sea border security.

As part of my job at RAND, I run one of five studies and analysis Federally Funded Research and Development Centers (FFRDCs) for the Department of Defense. These FFRDCs help the Secretary of Defense and other senior leaders address key policy challenges.

In this capacity, we routinely use performance measurement and modeling to provide decisionmakers with policy insights and options. For example, if the Secretary of Defense wanted to add a major new weapon system, we would help identify the most cost-effective set of requirements by using well developed models to estimate the effects on mission and cost as performance on different dimensions is varied. The Secretary of Defense also typically has sophisticated combat models at his disposal to help understand how the equipment will perform in operational situations.

We also use modeling and simulation at a more tactical level. For example, we can employ campaign models to help the Secretary to determine the best mix of weapon systems and forces to execute a major contingency operation or to estimate how outcomes would likely change with the introduction of new technologies, new operational concepts, or larger forces.

But now let's turn to our nation's analytic capability in the border security arena. What if Secretary Johnson wanted to know the effectiveness of adding 10,000 Border Patrol agents, or

---

[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. RAND testimonies record 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/CT415.html.

wanted to know the impact of a proposed border detection and surveillance system? We simply do not have all of the information and analytic tools in place to address these kinds of questions about the border.

It was these kinds of questions that I had in mind when I testified before House Homeland Security Committee's Subcommittees on Economic Security, Infrastructure Protection and Cybersecurity and Emergency Preparedness, Science and Technology at a field hearing in Washington State on August 8, 2006. In my testimony I noted:

> *"If there is an overarching theme to this testimony, it is that we have woefully underinvested in developing, evaluating, and refining a comprehensive and integrated border security strategy. We have invested in numerous border security programs and initiatives but the impacts and cost effectiveness of virtually all of these initiatives are poorly understood. We are virtually flying blind on a topic of critical national importance."*

Almost exactly eight years later, we are still struggling with some of these issues.

So, let me try to say it in a different way. We need investment in the basic policy science of homeland security. We need a strategy, data and technology infrastructure that lets us accomplish three things:

- Accurately and confidently measure and track the extent of relevant border activity, including illegal crossing activity and smuggling.
- Integrate that measurement and tracking data into frameworks that can be used to assess the effectiveness of border control policies.
- Integrate knowledge about effective border control policies into frameworks that help us understand the broader economic effects of border control.

Over the last decade, we have increased considerably the resources for border control with very little regard for the return on investment. Continuing the current investment patterns will be costly and provide progressively lower returns on investment.

Let me turn now to provide more detail on how we can get smarter about where to invest.

Measurement and Data Infrastructure

Effective border control begins with understanding why and how people cross the border. For purposes of the testimony today, I want to distinguish three different types of illegal border crossings.[4]

First are those crossings that are motivated principally the opportunity for a path to a better life in the U.S., often through the economic opportunity of working here, and more recently represented by the surge of children at the southern border. Second are those crossings that are primarily motivated by another kind of economic opportunity, that which comes from smuggling contraband across the border. Finally, the third kind of illegal border crossing is one that is intended to support terrorist activity. Research on individuals apprehended at the border reveals that economic opportunity is a primary motivation for illegal border crossings.[5] Indeed, more than two-thirds of the apprehended border crossers reported that economic opportunity was the primary reason for repeated attempts to cross the border.

The same policies do not necessarily work well against each type of motivation. Migration motivated by economic opportunity, for example, may best be controlled by a combination of border deterrence and labor market enforcement programs. In contrast, smuggling-related border crossings may be best addressed by deterrence and technological detection. Terrorism-related border crossings will demand yet another mix of policies.

We have the capability to estimate these different types of attempts at illegal border crossings. Among the approaches that are promising are:[6]

- **Capture-recapture methods**. These methods focus on the elapsed time between border apprehensions. The methods can be augmented by interviews with apprehended crossers to both understand crossing histories as well as intentions for the future.
- **Stratified sampling of border segments**. In this approach, the land border could be divided into low, medium and high risk zones, with enforcement resources allocated

[4] While there may be other motivations for illegal border crossings – such as family reunifications and flight from persecution – these three kinds of illegal border crossings comprise the bulk of illegal border crossings.
[5] Mark Grimes, Elyse Golub, Alexandra Durcikova, and Jay Nunamaker, "Reasons and Resolve to Cross the Line: A Post-Apprehension Survey of Unauthorized Immigrants along the U.S.-Mexican Border," National Center for Border Security and Immigration, University of Arizona, May 2013.
[6] Andrew R. Morral, Henry H. Willis and Peter Brownell, "Measuring Illegal Border Crossing Between Ports of Entry", RAND 2011.

based on risk. Crossing estimates can then be constructed by weighting apprehensions with enforcement intensity.

- **Population surveys.** One promising method is based on interviewing migrants about their crossing intentions as they pass through towns and choke points on the southern side of the border. A second is to start with a non-random sample of migrants in the US and, through networking or "snowballing," build a larger, more representative sample.
- **Synthetic and proxy measures**. Examples in this category include building estimates from visa overstays and extrapolating from changes in the cost of coyote (human smuggling) services.

However, as far as I can tell, these estimation methods have not been formally adopted, and to the extent they have been examined, they have not received sustained or sufficient support for continued development and refinement.

The first two methods – capture-recapture and stratified sampling – are especially relevant to smuggled goods. However, other than Office of National Drug Control Policy efforts to estimate illicit narcotic flows, I am not aware of any systematic effort to estimate other contraband over borders. In other words, a similar type of accounting framework needs to be built for contraband. That is, we need long-term data on how people attempt to smuggle goods over land borders and through other ports of entry.

Resource Allocation, Program Effectiveness and Adaptive Behavior

Once this foundation of data and information is established, the data can then be combined into models – mathematical representations – of how the border and border control policies work.

The types of questions we can answer once we have the data and models are:

- Should we do more of something?
- What policies or technologies can we substitute for approaches that are not working especially well?
- How do adversaries – particularly smugglers and terrorists – adapt their behavior to policy changes?

Recall the dilemma I posed for Secretary Johnson at the beginning of this testimony: how effective would it be to add 10,000 additional Border Patrol agents? Using the kind of data I

sketched out in the first section, we could not only assess the effectiveness of 10,000 additional agents, but give guidance on where and how to deploy them.[7]

Relatedly, machines and other instruments are often good substitutes for, or good complements to, people. A motion sensor, for example, might be better than having a person stand on guard duty. Night vision goggles, in contrast, might increase the effectiveness of people serving on guard duty. Again, using data and different modeling methods, we could make better decisions about when to use people, when to substitute technology, and when to use them together.

We know smugglers adapt their strategies to border security measures. One such example is the proliferation of tunnels under the U.S.-Mexican border. Another is the shift to small submarines. But, with better data, we might be better able to *predict* how behavior might adapt. At a minimum, we would likely detect the changes earlier in the adaptation cycle.

Finally, we tend to treat the different border types – air, land and sea – separately and discretely and this is likely a mistake. There is potentially tremendous value in integrating our understanding of how these borders interact. For example, greater stringency in detecting illicit cargo coming through ports may increase the incentives to use land smuggling routes.

By way of comparison, we as a nation fund such basic science data collection in many other policy realms including substance abuse (National Household Survey on Drug Abuse; Monitoring the Future; etc.). Twenty years ago, RAND used these data sources to model the cost-effectiveness of various interventions against illegal drugs, including source country control, border interdiction, domestic enforcement and treatment of heavy users. The insights that came from this work – namely that dollar for dollar treatment and prevention are more cost effective – would not have been possible without the data infrastructure and the modeling.

Understanding the Broader Economic and Social Implications of Border Control

Because our borders are so vital to commerce and the economy, policies implemented for border control purposes can propagate throughout the economy in unanticipated ways. Thus, it is not sufficient to know only whether a policy is effective at the narrow issue of border control. In many cases, we have to know something about a policy's broader economic and social effects before we can implement a policy with confidence.

---

[7] Joel B. Predd, Henry H. Willis, Claude Messan Setodji and Chuck Stelzner, Using Pattern Analysis and Systematic Randomness to Allocate U.S. Border Security Resources, RAND, 2012 is a recent report on using modeling to guide resource allocation.

Consider some examples.

Sometimes the effects of border control policies are relatively diffuse and difficult to document. The scale and complexity of US ports provides an example. Each year, approximately $500 billion of goods enter and $200 billion exit the United States through ports. Among this is cargo that is perishable, goods that are critical inputs into manufacturing processes, and seasonal materials that have limited periods of retail relevance. Thus, changes to the intensity, cost and speed of cargo security inspections can have broad and highly dispersed effects.

In other cases, the consequences of border control may be difficult to detect. For example, visas became a target for reform in part because all 19 of the terrorists involved in the 9/11 attacks were in the United States on legitimate visas. Residents of many countries can travel to the United States without obtaining a visa, but those traveling from other nations, such as Pakistan, Saudi Arabia, and Yemen, must obtain one by providing extensive documentation (of the individual and, in some cases, family members, business associates, and the sponsor) that is investigated using homeland security, intelligence, and law enforcement databases and resources, and undergoing an in-person consular interview. By making it harder to come to the United States, we deter not only terrorists but also an unknown number of legitimate travelers—foreign tourists, foreign students, and qualified foreign workers—whose presence provides great benefits to our economy and the vibrancy of our culture.

In still other cases, border enforcement affects issues as fundamental to U.S. society as employment. Labor market enforcement is one example. Right now, labor market enforcement is relatively weak. For example, there were 639 criminal indictments and 586 convictions related to worksite enforcement investigations in 2011.[8] E-Verify, which allows employers to check the work eligibility of their employees, is currently voluntary. There are significant errors in the E-Verify database, which means that people legitimately able to work in this country are sometimes rejected. This is one reason that making E-Verify mandatory is a potentially risky step.

One mechanism for strengthening E-Verify and reducing errors is to have employers submit their verified I-9 forms to E-Verify. Employers must fill out an I-9 form for each new employee. Completion of this form certifies that the hiring authority has confirmed an applicant's identity and eligibility to work by examining a document such as a passport. However, employers are only required to maintain the I-9 information at their offices. If these documents were instead submitted as part of E-Verify, it would greatly increase the intelligence and information that DHS

[8] Andorra Bruno, "Immigration-Related Worksite Enforcement: Performance Measures", Congressional Research Service, May 10, 2012.

has about illegal employment patterns and it might deter employers from being willing to hire improperly documented employees. This approach is not without controversy, as it imposes a new compliance requirement on employers.

These opportunity costs – and many others – need to be accounted for in a national border control strategy.

Next Steps and Conclusions

Various pieces of legislation, including HR 1417 in the 113th Congress, have called for the development of this critical analytical capability, though none that I am aware of have been signed into law. HR 1417 required:

> *"estimates of the relative cost effectiveness of various border security strategies and operations, including deployment of personnel and technology, and construction of new physical and virtual barriers."*

It is encouraging to see a call for this kind of modeling to inform decisions about where and how to invest. To my knowledge, no such modeling, and no such approach to border security, is currently being undertaken.

Finally, I would be remiss if I did not note how difficult it is to conduct effective policy analysis in this area.[9] It is difficult to get access to data to conduct effective modeling. It is also difficult to publish in the scientific literature in this area. The ability to get data and to publish are what help attract bright minds to policy challenges. But publishing is also important for another reason: by submitting the work to public and scholarly scrutiny, we ensure that the work is accurate. While I realize that border security presents many important security challenges, too often contracts with the Department of Homeland Security place unnecessary and unproductive restrictions on public, academic, and policy discussion of these important issues.

Let me close by repeating something I noted in my 2006 testimony: there is no single programmatic fix. Border security will be achieved through a network of mutually reinforcing, and to some extent redundant, layers of defenses. The solutions will span the bounds of cabinet agencies in the federal government. As a consequence, we need to consider not just the effects of individual programs, but the interaction effects of multiple programs. It is important that we get

[9] Alicia Carriquiry and Malay Majmundar, editors, "Options for Estimating Illegal Border Entries at the U.S.-Mexico Border," Committee on National Statistics, National Research Council.

an analytic framework in place soon so that we can begin to make more informed decisions about border control resource issues.

Jack Riley is RAND vice president of the National Security Research Division and director of National Defense Research Institute (NDRI). NDRI is a Federal Funded Research and Development Center which supports the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Department of the Navy, the Defense Agencies and the Defense Intelligence Community. From March 2008 to January 2010, Riley was associate director of NDRI, and before then, he served as associate director of RAND Infrastructure, Safety, and Environment. Much of his recent work has focused on security sector reform, including analyses of Afghanistan, Liberia, Mexico, and the Palestinian territories. In addition, he has conducted extensive work on homeland security, border security, and law enforcement and crime control, including assessments of passenger rail and airport security, implementation of a gun crime reduction demonstration program, and analyses of major law enforcement initiatives and reforms at the local, state, and national levels.

He has testified before Congress on multiple occasions on transportation security and border security. Recent publications include *Effective Policing for 21st-Century Israel; Air Travel Security Since 9/11; Developing a Defense Sector Assessment Rating Tool;* and *Security in Mexico: Implications for U.S. Policy Options.* Riley's speech, "Moving Toward a Sustainable U.S. Defense Budget," is also available as a RAND publication. From 1995 to 1999, Riley was with the U.S. Department of Justice, where he conducted research and managed programs addressing a wide variety of issues, including domestic terrorism, immigration reform, substance abuse trends, violent crime, offender monitoring, and law enforcement reforms. Riley received his BA (economics and Russian) from the University of Michigan; a certificate of language specialization from Leningrad State University; his MS (foreign service) from Georgetown; and his PhD (public policy analysis) from the RAND Graduate School.

Chairman BUCSHON. Thank you very much.

I now recognize Mr. Maurer for five minutes for his testimony.

TESTIMONY OF MR. DAVID C. MAURER, DIRECTOR, HOMELAND SECURITY AND JUSTICE, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. MAURER. Good morning, Chairman Bucshon, Chairman Broun, Chairman Smith, Ranking Member Lipinski, Ranking Member Maffei, and Members and staff. I am pleased to be here this morning to talk about the results of our recently issued work looking at research and development at the Department of Homeland Security and how those efforts are being used to enhance border security.

R&D matters at DHS for a couple of reasons. First, the taxpayers provide DHS over $1 billion a year to support research and development. For that reason alone, the Department needs to ensure its R&D activities work as planned. R&D can also help DHS better execute its various missions. For example, improved technology to detect people or nuclear material helps DHS secure the border and ultimately the homeland.

DHS has made important strides in recent years towards taking a more strategic approach. For example, the Science and Technology Directorate has a strategic plan, periodically reviews its portfolio of projects, and has developed new ways to coordinate with other DHS components. That last point is especially important since S&T strives to conduct its R&D work side by side with the eventual end users. But that said, DHS clearly has a lot of work ahead to bring coherence and structure to its research and development efforts.

Our work over the past two years identified three key areas where DHS needs to improve. We found that DHS needed to define R&D, do a better job tracking R&D, and improve how it coordinates R&D. I will briefly expand on these three points.

In September 2012, we reported that DHS lacked a common definition of research and development, and we found a lot of activity across the Department that could be considered R&D, and by law, S&T is responsible for coordinating and overseeing all of it, but they can't do that if the various DHS components aren't working from the same definition and agree on what should be coordinated. Our work also found several problems in DHS's efforts to essentially track R&D. As it turned out, DHS struggled to answer basic questions such as how much are you spending, which components are doing R&D, what projects are currently underway, and do completed projects meet the needs of their customers. For example, we found that DHS did not know how much its components invested in R&D, and that makes it really difficult to oversee activities across the entire Department. This inability to centrally track R&D also places DHS at risk of overlapping and duplicative efforts. We identified 35 instances where contracted R&D activity in one component overlapped with another.

Our work also identified problems in DHS's ability to coordinate R&D. There are several R&D coordination mechanisms within DHS but they need to work better. For example, the report we issued last year on border and maritime found a mixed picture.

The good news is that the Domestic Nuclear Detection Office and the Coast Guard regularly reach out to end users of their completed R&D Projects. However, S&T lacked any formal approach to follow-up with the end users of its deliverables. S&T's customers are also much more likely to report that S&T deliverables did not meet end-user needs, and in some instances, we were unable to locate an end user for an S&T project. For example, S&T spent more than $1 million on a project to enhance CBP's ability to track maritime vessels without having a specific customer at CBP. Our recent work also found problems in DHS's coordination of R&D work with the national labs.

So what is DHS doing to better define, track and coordinate R&D? On the plus side, the Department now has a common definition for R&D, and that is an important first step. However, while DHS has taken some actions, they are still not sufficient to address our recommendations to improve how they track and coordinate R&D, and that is important because clearly defined, closely tracked and well-coordinated R&D activities will help translate state-of-the-art science into usable tools that can help enhance the security of our borders. We will keep the Committee informed on the Department's ongoing efforts to address our recommendations.

Mr. Chairman, thank you. That concludes my opening remarks. I look forward to your questions.

[The prepared statement of Mr. Maurer follows:]

United States Government Accountability Office

Testimony
Before the Subcommittee on Research and Technology and the Subcommittee on Oversight, Committee on Science, Space, and Technology, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. ET
Thursday, July 31, 2014

DEPARTMENT OF HOMELAND SECURITY

Continued Actions Needed to Strengthen Oversight and Coordination of Research and Development

Statement of David C. Maurer, Director
Homeland Security and Justice

GAO-14-813T

GAO Highlights

Highlights of GAO-14-813T, a testimony before the Subcommittee on Research and Technology and the Subcommittee on Oversight, Committee on Science, Space, and Technology, House of Representatives

July 31, 2014

DEPARTMENT OF HOMELAND SECURITY

Continued Actions Needed to Strengthen Oversight and Coordination of Research and Development

Why GAO Did This Study

Conducting R&D on technologies for detecting, preventing, and mitigating terrorist threats is vital to enhancing the security of the nation. Since its creation, DHS has spent billions of dollars researching and developing technologies used to support its missions including securing the border, and detecting nuclear material among others. Within DHS, S&T conducts and is responsible for coordinating R&D across the department. Other components also conduct R&D to support their respective missions.

This statement discusses (1) how much DHS invests in R&D and the extent to which DHS has policies and guidance for defining and overseeing its R&D efforts across the department, (2) the extent to which R&D is coordinated across DHS, and (3) the results of DHS border and maritime security R&D efforts and the extent to which DHS has obtained feedback on these efforts. This statement is based on GAO's previously issued work from September 2012 to September 2013, and selected updates conducted in July 2014 on the status of GAO's prior recommendations. To conduct the updates, GAO reviewed agency documentation.

What GAO Recommends

In its prior reports, GAO recommended, among other things, that DHS develop policies and guidance for defining, overseeing, coordinating, and tracking R&D activities across the department; and that S&T collect and evaluate feedback from its customers. DHS concurred with GAO's recommendations and has actions underway to address them.

View GAO-14-813T and GAO-13-732. For more information, contact Dave Maurer at (202) 512-9627 or maurerd@gao.gov.

What GAO Found

In September 2012, GAO reported that the Department of Homeland Security (DHS) did not know the total amount its components invested in research and development (R&D) and did not have policies and guidance for defining R&D and overseeing R&D resources across the department. According to DHS, its Science & Technology Directorate (S&T), Domestic Nuclear Detection Office (DNDO), and Coast Guard were the only components that conducted R&D, and GAO found that these were the only components that reported budget authority, obligations, or outlays for R&D activities to the Office of Management and Budget. However, GAO identified an additional $255 million in R&D obligations made by other DHS components. At the time of GAO's review, DHS reported it was difficult to identify all R&D investments across the department because DHS did not have a department wide policy defining R&D or guidance directing components how to report all R&D activities. GAO recommended that DHS develop policies to assist components in better understanding how to report R&D activities and better position DHS to determine R&D investments. DHS concurred with the recommendation and, as of July 2014, had updated its guidance to include a definition of R&D but had not yet determined the most effective path to guide R&D across the department. GAO will continue to monitor DHS's efforts to develop its approach for overseeing R&D at the department.

GAO also reported in September 2012 that S&T had taken some steps to coordinate R&D efforts across DHS, but the department's R&D efforts were fragmented and overlapping, which increased the risk of unnecessary duplication. GAO recommended that DHS develop a policy defining roles and responsibilities for coordinating R&D and establish a mechanism to track all R&D projects to help DHS mitigate existing fragmentation and overlap and reduce the risk of unnecessary duplication. DHS concurred with the recommendation. As of July 2014, S&T has not developed new policy guidance but is conducting portfolio reviews across the department, as directed by the fiscal year 2013 appropriations act, aimed at coordinating R&D activities. GAO will continue to monitor DHS's efforts to develop a policy to better coordinate and track R&D activities at the department.

In September 2013, GAO reported that DHS border and maritime R&D components reported producing 97 R&D deliverables from fiscal year 2010 through 2012 at an estimated cost of $177 million. GAO found that the type of border and maritime R&D deliverables produced by S&T, the Coast Guard, and DNDO varied, and R&D customers GAO met with had mixed views on the impact of the deliverables. These deliverables included knowledge products and reports, technology prototypes, and software. For example, S&T developed prototype radar and video systems for use by Border Patrol. However, GAO reported that S&T had not established timeframes for collecting and evaluating feedback on the extent to which deliverables met customers' needs. GAO recommended that S&T collect such feedback from its customers to better determine the usefulness and impact of its R&D projects and deliverables and make better-informed decisions regarding future work. As of July 2014, DHS had taken steps to address this recommendation, including making plans to gather customer feedback. GAO will continue to monitor DHS's efforts in this area.

Chairman Bucshon, Chairman Broun, Ranking Member Lipinski, Ranking Member Maffei, and Members of the Committee:

I appreciate the opportunity to testify today about our prior work discussing the results of the Department of Homeland Security's (DHS) research and development (R&D) efforts, including the extent to which its R&D efforts are coordinated within DHS and the results of DHS's border and maritime security R&D efforts. According to the Office of Management and Budget (OMB), R&D activities comprise creative work undertaken on a systematic basis in order to increase the stock of knowledge, including knowledge of man, culture, and society, and the use of this stock of knowledge to devise new applications.[1] R&D is further broken down into the categories of basic research, applied research, and development.[2]

Conducting R&D on technologies for detecting, preventing, and mitigating terrorist threats is vital to enhancing the security of the nation. DHS, through its Science and Technology Directorate (S&T) and other components, conducts research, development, testing, and evaluation of new technologies that are intended to achieve a range of homeland security goals, including detecting and preventing the unauthorized entry of persons or contraband into the United States; strengthening efforts to prevent and respond to nuclear, biological, explosive, and other types of attacks; and securing U.S. ports and inland waterways. DHS S&T has responsibility for coordinating and integrating all R&D activities of the department, as provided by the Homeland Security Act of 2002.[3]

[1]OMB Circular No. A-11 Section 84.4. This definition includes administrative expenses for R&D, but excludes physical assets for R&D (such as R&D equipment and facilities), routine testing, quality control mapping, collection of general-purpose statistics, experimental production, routine monitoring and evaluation of an operational program and the training of scientific and technical personnel.

[2]According to OMB, basic research is a systematic study directed toward a fuller knowledge or understanding of the fundamental aspects of phenomena and of observable facts without specific applications towards processes or products in mind. Applied research is a systematic study to gain knowledge or understanding to determine the means by which a recognized and specific need may be met. Development is a systematic application of knowledge or understanding, directed toward the production of useful materials, devices, and systems or methods, including design, development, and improvement of prototypes and new processes to meet specific requirements. OMB Circular No. A-11 Section 84.

[3]Pub. L. No. 107-296, § 302 (12),116 Stat. 2135, 2163-64 (codified as amended at 6 U.S.C. § 182 (12)).

Although S&T conducts R&D and has responsibility for coordinating R&D, other DHS components, including the Domestic Nuclear Detection Office (DNDO) and the U.S. Coast Guard, conduct R&D in support of their respective missions. Since it began operations in 2003, DHS, through both S&T and other components, has spent billions of dollars researching and developing technologies used to support a wide range of missions.

With respect to border and maritime R&D specifically, S&T's Borders and Maritime Security Division (BMD) is responsible for most of S&T's border and maritime related R&D and its primary DHS customer is U.S. Customs and Border Protection (CBP). Within S&T, the Office of University Programs manages the DHS Centers of Excellence, which constitute a network of universities that conduct research for DHS component agencies, with two centers dedicated specifically to border and maritime R&D. DNDO conducts R&D applicable to border and maritime security as it relates to its mission of detecting the use of an unauthorized nuclear explosive device, fissile material, or radiological material in the United States.[4] The U.S. Coast Guard's R&D efforts support all of the various Coast Guard missions, such as search and rescue, migrant interdiction, and marine safety.

My testimony today addresses (1) how much DHS invests in R&D and the extent to which it has policies and guidance for defining R&D and overseeing R&D resources and efforts across the department; (2) the extent to which R&D is coordinated within DHS to prevent overlap, fragmentation, and unnecessary duplication across the department; and (3) the results of DHS's border and maritime security R&D and the extent to which DHS obtained and evaluated feedback on these efforts.

This statement is based on our previous reports and testimonies issued from September 2012 to September 2013 with selected updates conducted in July 2014 related to S&T's efforts to better manage and

[4]DNDO was established by National Security Presidential Directive 43, Homeland Security Presidential Directive 14, and the Security and Accountability for Every Port Act of 2006 (SAFE Port Act). Pub. L. No. 109-347, § 501(a), 120 Stat. 1884, 1932 (codified at6 U.S.C. §§ 591-596).

coordinate its border and maritime R&D efforts.[5] To conduct our earlier work, among other things, we analyzed data related to DHS's R&D budget authority for fiscal years 2010 through 2013, R&D contracts issued by components to private industry and universities for fiscal years 2007 through 2011, and the Department of Energy's (DOE) national laboratories from fiscal years 2010 through 2012 to identify how much DHS components obligated for R&D-related work at the national laboratories. We also met with R&D project managers and customers. For the selected updates, we reviewed agency documentation on DHS's progress in implementing our prior recommendations. The reports cited provide detailed explanations of our scope and methodology.[6] We conducted this work in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

DHS Does Not Know Its Total Investment in R&D, but Has Taken Some Steps to Update Guidance

In September 2012, we found that DHS did not know how much its components invested in R&D, making it difficult to oversee R&D efforts across the department. According to DHS budget officials, S&T, DNDO, and the U.S. Coast Guard were the only components that conducted R&D and we found that they were the only components that reported budget authority, obligations, or outlays for R&D activities to OMB as part of the budget process. However, we reported that the data DHS submitted to OMB underreported DHS's R&D obligations because DHS components obligated money for R&D contracts that were not reported to OMB as

[5]GAO, *Department of Homeland Security: Oversight and Coordination of Research and Development Should Be Strengthened,* GAO-12-837 (Washington, D.C.: Sept.12, 2012). GAO-13-279SP. GAO, *Department of Homeland Security: Opportunities Exist to Strengthen Efficiency and Effectiveness, Achieve Cost Savings, and Improve Management Functions,* GAO-13-547T (Washington, D.C.: April 26, 2013). GAO, *Government Efficiency and Effectiveness: Opportunities to Reduce Fragmentation, Overlap, and Duplication through Enhanced Performance Management and Oversight,* GAO-13-590T (Washington, D.C.: May 22, 2013). GAO, *Department of Homeland Security: Opportunities Exist to Better Evaluate and Coordinate Border and Maritime Research and Development,* GAO-13-732 (Washington, D.C.: Sept. 25, 2013). GAO, *Department of Homeland Security: Oversight and Coordination of Research and Development Efforts Could be Strengthened,* GAO-13-766T (Washington, D.C.: (July 17, 2013).

[6]GAO-12-837 and GAO-13-732.

R&D. Specifically, for fiscal year 2011, we identified an additional $255 million in R&D obligations by other DHS components. These obligations included DHS components providing S&T with funding to conduct R&D on their behalf and components obligating funds through contracts directly to industry, universities, or with DOE's national laboratories for R&D.

Further, we found that the data for fiscal years 2010 through 2013 DHS submitted to OMB also underreported DHS's R&D budget authority and outlays because DNDO did not properly report at least $293 million in R&D budget authority and at least $282 million in R&D outlays.[7] We reported that DHS budget officials agreed that DHS underreported its R&D spending and when asked, could not provide a reason why the omission was not flagged by DHS review.

In addition, in our 2012 report, we found that DHS's R&D budget accounts included a mix of R&D and non-R&D spending. For fiscal year 2011, we estimated that 78 percent of S&T's Research, Development, Acquisition, & Operations account, 51 percent of DNDO's Research, Development, & Operations account, and 43 percent of the Coast Guard's R&D budget account funded R&D activities. As a result, this further complicated DHS's ability to identify its total investment in R&D.

We also reported in September 2012 that DHS did not have a department wide policy defining R&D or guidance directing components how to report R&D activities. As a result, we concluded that it was difficult to identify the department's total investment in R&D, which limited DHS's ability to oversee components' R&D efforts and align them with agency wide R&D goals and priorities, in accordance with Standards for Internal Control in the Federal Government.[8] DHS officials told us at the time that DHS used OMB's definition of R&D, but the definition was broad and its application may not be uniform across components, and thus, R&D investments may not always be identified as R&D. We found that the variation in R&D definitions may contribute to the unreliability of the reporting mechanisms

[7]At the time of our report, budget figures for fiscal year 2013 were agency estimates.

[8]*Standards for Internal Control in the Federal Government* state that policies and mechanisms are needed to enforce management's directives, such as the process of adhering to requirements for budget development and execution and to ensure the reliability of those and other reports for internal and external use. GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: Nov. 1999).

for R&D investments in budget development and execution, as discussed above.

We recommended that DHS develop and implement policies and guidance for defining and overseeing R&D at the department that include, among other things, a well-understood definition of R&D that provides reasonable assurance that reliable accounting and reporting of R&D resources and activities for internal and external use are achieved. DHS agreed with our recommendation and stated that it planned to evaluate the most effective path forward to guide uniform treatment of R&D across the department in compliance with OMB rules and was considering a management directive, multi-component steering committee, or new policy guidance to help better oversee and coordinate R&D. As of July 2014, DHS has updated its guidance to include a definition of R&D, but as discussed in more detail below efforts to develop a specific policy outlining R&D roles and responsibilities and a process for coordinating R&D with other offices remain ongoing and have not yet been completed.[9] We will continue to monitor DHS's efforts to implement these recommendations.

S&T Has Taken Some Actions to Coordinate R&D across DHS, but R&D Activities are Fragmented and Overlapping

We reported in September 2012 that the Homeland Security Act of 2002 provides S&T with the responsibility for, among other things, coordinating and integrating all research, development, demonstration, testing, and evaluation activities within DHS and establishing and administering the primary R&D activities of the department.[10] S&T developed coordination practices that fall into four general categories: (1) S&T component liaisons, (2) R&D agreements between component heads and S&T, (3) joint R&D strategies between S&T and components, and (4) various R&D coordination teams made up of S&T and component project managers, which are discussed in detail in our 2012 report and 2013 testimony.[11]

Despite S&T's efforts to coordinate R&D activities, in September 2012, we reported that R&D at DHS was inherently fragmented because several components within DHS—S&T, the Coast Guard, and DNDO—were each

[9]GAO, *Biosurveillance: Observations on the Cancellation of BioWatch Gen-3 and Future Considerations for the Program*, GAO-14-267T (Washington D.C.: June 10, 2014).

[10]6 U.S.C. § 182(11)-(12).

[11]GAO-13-766T

given R&D responsibilities in law, and other DHS components may pursue and conduct their own R&D efforts as long as those activities are coordinated through S&T. Fragmentation among R&D efforts at DHS may be advantageous if the department determines that it could gain better or faster results by having multiple components engage in R&D activities toward a similar goal; however, it can be disadvantageous if those activities are uncoordinated or unintentionally overlapping or duplicative. Specifically, we found at least six department components involved in R&D activities in our review of data on about 15,000 federal procurement contract actions coded as R&D taken by DHS components from fiscal years 2007 through 2012. We examined 47 R&D contracts awarded by these components—selected because they appeared to have similar activities to another contract—and found 35 instances among 29 contracts in which the contracts overlapped with activities conducted elsewhere in the department. Taken together, these 29 contracts were worth about $66 million. In one example of the overlap, we found that two DHS components awarded five separate contracts that each addressed detection of the same chemical.

While we did not identify instances of unnecessary duplication among these contracts, in September 2012 we found that DHS had not developed a policy defining who is responsible for coordinating R&D activities at DHS that could help prevent overlap, fragmentation, or unnecessary duplication and did not have tracking mechanisms or policies to help ensure that overlap is avoided and efforts are better coordinated consistent with Standards for Internal Control in the Federal Government.[12] S&T officials told us at the time that a process did not exist at DHS or within S&T to prevent overlap or unnecessary duplication but that relationships with components mitigate that risk. They also stated that S&T has improved interactions with components over time. We concluded that the existence of overlapping R&D activities coupled with the lack of policies and guidance defining R&D and coordination processes was an indication that not all R&D activities at DHS were

[12]GAO's *Standards for Internal Control in the Federal Government* state that policies and procedures ensure that the necessary activities occur at all levels and functions of the organization—not just from top-level leadership. This ensures that all levels of the organization are coordinating effectively and as part of a larger strategy. Additionally, internal control standards provide that agencies should communicate necessary information effectively by ensuring that they are communicating with, and obtaining information from, external stakeholders that may have a significant impact on the agency achieving its goals.

coordinated to ensure that R&D is not unnecessarily duplicative. We also found in September 2012 that neither DHS nor S&T tracked all ongoing R&D projects across the department, including R&D activities contracted through the national laboratories. As part of our review, we identified 11 components that reimbursed the national laboratories for R&D from fiscal years 2010 through 2012, but S&T's Office of National Laboratories could not provide us with any information on those activities and told us it did not track them. According to S&T, the Office of National Laboratories' ability to provide information on activities across the department is limited by components inconsistently operating within the defined process for working with the national laboratories.[13]

As a result, we recommended that DHS develop and implement policies and guidance for overseeing R&D that includes, among other things, a description of the department's process and roles and responsibilities for overseeing and coordinating R&D investments and efforts, and a mechanism to track existing R&D projects and their associated costs across the department. DHS agreed with our recommendation and stated at the time that S&T was implementing a collaborative, end-user focused strategy to coordinate and interact with components to better ensure S&T's efforts aligned with components' needs and that it was considering developing new policy guidance for R&D activities across the department. As of July 2014, DHS has not developed new policy guidance but is conducting portfolio reviews across the department, as directed in committee reports accompanying the fiscal year 2013 DHS appropriation act, aimed at coordinating R&D activities.[14] Fully implementing our recommendation to develop a policy that defines roles and responsibilities for coordinating R&D and coordination processes, as well as a mechanism that tracks all DHS R&D projects, could better position DHS to mitigate the risk of overlapping and unnecessarily duplicative R&D projects. We will continue to monitor DHS's efforts to develop a policy to better coordinate and track R&D activities at the department.

[13]The Homeland Security Act of 2002 gave DHS the authority to use DOE laboratories to conduct R&D and established S&T's Office of National Laboratories to be responsible for coordinating and using the DOE national laboratories. Pub. L. No. 107-296, § 309, 116 Stat. 2135, 2172 (2002) (codified at 6 U.S.C. § 189). Additionally, DHS Directive 143 further directs ONL to serve as the primary point of contact to recommend contracting activity approval for work by the national laboratories, and review all statements of work issued from DHS and directed to the national laboratories.

[14]See S. Rep. No. 112-169, at 15-16 (2012).

S&T Has Taken Steps to Obtain Feedback and Evaluate the Impact of Its Border and Maritime R&D Efforts

Costs and Types of Completed Border and Maritime R&D Projects Varied

In September 2013, we reported that DHS S&T, Coast Guard, and DNDO reported producing 97 Border and Maritime R&D deliverables at an estimated cost of $177 million from fiscal years 2010 through 2012. The type of border and maritime R&D deliverables produced by these R&D entities were wide-ranging in their cost and scale, and included knowledge products and reports, technology prototypes, and software.[15] For example:

- **Knowledge products or reports:** One of the DHS Centers of Excellence developed formulas and models to assist in randomizing Coast Guard patrol routes and connecting networks together to assist in the detection of small vessels.
- **Technology prototypes:** S&T BMD developed prototype radar and upgraded video systems for use by Border Patrol agents and a prototype scanner to screen interior areas of small aircraft without removing panels or the aircraft skin.
- **Software:** DNDO developed software that extracts data from radiation portal monitors and uses the data to improve algorithms used in detecting radioactive material.

As we reported in September 2013, R&D customers we met with had mixed views on the impact of the R&D deliverables they received. For example, we reviewed 20 S&T BMD deliverables produced from fiscal years 2010 through 2012 at a cost of $28.7 million. We found that the customers of 7 deliverables stated that the deliverables met their office's needs, customers of 7 did not, customers of 4 did not know, and

[15]A complete list of all 97 projects for fiscal years 2010 through 2012 and their costs and project type can be found in Appendix I of GAO-13-732.

customers for 2 could not be identified.[16] For example, customers within CBP's Office of Technology Innovation and Acquisition reported that S&T's analysis and test results on aircraft-based use of wide area surveillance technology helped CBP to make a decision on whether it should pursue acquiring such technology. In cases where customers said that the deliverables were not meeting their needs, the customers explained that budget changes, other ongoing testing efforts, or changes in mission priorities were the reasons deliverables had not met their needs, and customers pointed out that their relationship with S&T had been positive and highly collaborative. In other cases, customers pointed out that while the deliverable had not been used as intended, it informed their office's decision making and helped to rule out certain technologies as possibilities. In this regard, the customers felt the R&D was successful, despite the fact that the deliverable had not or was not being used.

S&T BMD officials explained that some of its older projects did not have identifiable customers because its former process for selecting projects created the potential to engage in R&D without a clear commitment from the customer. In February 2012, S&T issued a new project management guide that requires project managers to specify the customer by office and name, and to describe customer support for the project, including how the customer has demonstrated commitment for and support of the project. S&T officials said they believed this new process would prevent future R&D funding from going towards projects without a clear customer.

Additionally, we reported that from fiscal year 2010 through fiscal year 2012, DNDO produced 42 deliverables at a cost of $115.9 million, which included 6 discontinued projects and 36 projects that were either transitioned to the next phase of R&D or were completed. DNDO R&D is different from the R&D of S&T for many reasons. For one, a DNDO project may start at a basic research level, and may end up being merged into other similar efforts in order to achieve a higher project goal. In these cases, the R&D customers are DNDO project managers rather than another DHS customer, such as CBP. We discussed 5 DNDO R&D deliverables at various R&D phases with DNDO officials—4 of which were deliverables from ongoing or completed projects and 1 of which was a discontinued project. Two of the 5 projects we discussed had moved from

[16]This figure does not include projects from the S&T Office of University Programs, which reported completing 18 border and maritime related projects at a cost of $6.1 million.

early-stage R&D into other projects further along in DNDO's project management process. Two of the 5 projects were completed, with 1 project that was reported to have provided information that informed furthered DNDO decision-making and the other project resulting in a commercialized product. With regard to the 1 discontinued project, DNDO officials said that the particular project's technology was determined to be too expensive to continue pursuing.

S&T Did Not Gather and Evaluate Feedback

We reported that although S&T project managers sought feedback from their customers during the execution of projects, S&T did not gather and evaluate feedback from its customers to determine the impact of its completed R&D efforts and deliverables, making it difficult to determine if the R&D met customer needs. Further, in some cases, the customer of S&T's R&D was not clear or the results of the R&D were unknown. For example, a CBP customer identified by S&T was aware of two R&D deliverables that S&T said were transitioned to his office, but the official was unable to provide additional information on the project's impact. According to S&T officials, since they deal with multiple DHS components and are not within the same agencies as its customers, it is sometimes difficult to identify who the customer of the R&D is and also difficult to determine what the impact of the R&D was. S&T officials also stated that in S&T's 2012 update to its project management guide, in its project closeout process, S&T had included a step to collect feedback from all relevant customers and a template for collecting this feedback.

While we found in September 2013 that S&T had developed a process and template to collect feedback at the end of each project and incorporated this into its project management plan, we also found that it did not plan to survey customers each time it provides a deliverable to the customer. This is relevant because S&T projects are often conducted over several years before they are concluded and these projects also often produce multiple deliverables for a customer over many years that are designed to meet a specific operational need. For example, a Ground Based Technologies project began in fiscal year 2006 and was slated to continue through fiscal year 2018. During this period, S&T provided multiple R&D deliverables to CBP—including test results comparing different ground based radar systems. The National Academy of Sciences has stated that feedback from both R&D failures and successes may be

communicated to stakeholders and used to modify future investments.[17] At the time of our report, S&T had not established timeframes and milestones for collecting and evaluating feedback from its customers on the extent to which the deliverables it provides were meeting its customer's needs.

As a result, we recommended that S&T establish timeframes and milestones for collecting and evaluating feedback from its customers to determine the usefulness and impact of both its R&D projects and project deliverables, and use it to make better-informed decisions regarding future work. S&T officials concurred with the recommendation at the time of our review, and reported that it was developing R&D strategies with DHS components, which would include a strategic assessment of components' R&D needs and updated annually on the basis of customer feedback. As of July 2014, S&T has completed strategic plans with Border Patrol, the Transportation Security Administration (TSA), and the Secret Service. Further, at the time of our review, S&T reported that it was developing a new project management guide to improve R&D management at all stages of development, and that the guide would include a template for project managers to use to gather customer feedback on a more consistent basis. In November 2013, S&T finalized its guide which includes a customer survey template to obtain feedback on the quality, timeliness, and relevance of a deliverable, as well as detailed descriptions of actions project managers should take throughout a project to ensure the R&D is aligned with customer needs. We will continue to review the implementation of these actions and to determine whether they fully address the intent of our recommendation.

DHS Border and Maritime R&D Agencies Have Taken Action to Improve Internal and External R&D Coordination

In September 2013, we also reported that S&T's BMD, the Coast Guard, and DNDO reported taking a range of actions to coordinate with one another and their customers to ensure that R&D is addressing high priority needs. Officials from BMD identified several ways in which it coordinated R&D activities with its customers, which are primarily offices within CBP. For example, BMD officials reported having a person detailed to CBP's Office of Technology Innovation and Acquisition and identified its integrated product teams, such as its cross border tunnel threat team,

[17]National Academy of Sciences, *Best Practices in Assessment of Research and Development Organizations*.2012.

and jointly funded projects as ways in which the division worked to ensure its R&D efforts were coordinated with CBP. We also found that opportunities existed for DHS to enhance coordination with universities conducting R&D on its behalf. Specifically, we reported that the S&T Office of University Programs could help ensure that the approximately $3 million to $4 million a year dedicated to each university center is used more effectively by more carefully considering data needs, potential access issues, and potential data limitations with its federal partners before approving projects. We recommended that S&T ensure design limitations with regard to data reliability, accessibility, and availability are reviewed and understood before approving Center of Excellence R&D projects. S&T Office of University Programs officials concurred with the recommendation and discussed the variety of ways in which centers and DHS components collaborate and share information. Office of University Programs officials stated that the office's process for soliciting research topics and evaluating proposals is good and that it keeps the centers flexible. However, officials from DHS's primary land border security Center of Excellence reported challenges with respect to a lack of clarity regarding protocols for access to DHS information when conducting R&D. Specifically, officials from this center reported that they have been regularly unable to obtain data from CBP to complete research it was conducting on CBP's behalf, which resulted in delays and terminated R&D projects.

Given the challenges raised by officials from universities leading the R&D for land border security, we recommended that S&T conduct a more rigorous review of potential data-related challenges and limitations at the start of a project in order to help R&D customers (such as CBP) identify data requirements and potential limitations up front so that money is not allocated to projects that potentially cannot be completed. In concurring with our recommendation, S&T Office of University Programs officials agreed that making sure their clients take additional steps to identify data requirements up front could help address these challenges and following our review had started taking steps to address the recommendation. For instance, in September 2013, the Office of University Programs reported that it was working to develop standard guidelines and protocols that would apply to all of its centers of excellence. These protocols were to describe how data sets must be modified to enable their use in open-source research formats. In March 2014, the Office of University Programs and the National Center for Border Security and Immigration, a DHS S&T Center of Excellence, co-hosted a workshop to identify common problems the centers have in accessing data from DHS, understand DHS constraints in sharing data, and develop best practices

for requesting and sharing data between the centers of excellence and DHS. We believe this is a step in the right direction and should move S&T closer toward meeting the intention of our recommendation. We will continue to monitor DHS's efforts in this area.

Chairman Bucshon, Chairman Broun, Ranking Member Lipinski, Ranking Member Maffei, and members of the committee, this completes my prepared statement. I would be happy to respond to any questions you may have at this time.

GAO Contact and Staff Acknowledgements

If you or your staff members have any questions about this testimony, please contact me at (202) 512-9627 or Maurerd@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Key contributors to this statement include Adam Hoffman, Assistant Director; Aditi Archer, and Charlotte Gamble. Francis Cook, Michele Fejfar, Emily Gunn, Richard Hung, Gary Malavenda, and Linda Miller also made contributions to this testimony.

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission	The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."
Order by Phone	The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm. Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537. Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.
Connect with GAO	Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.
To Report Fraud, Waste, and Abuse in Federal Programs	Contact: Website: http://www.gao.gov/fraudnet/fraudnet.htm E-mail: fraudnet@gao.gov Automated answering system: (800) 424-5454 or (202) 512-7470
Congressional Relations	Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548
Public Affairs	Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

Please Print on Recycled Paper.

GAO
U.S. GOVERNMENT
ACCOUNTABILITY OFFICE

David Maurer, Director Homeland Security and Justice

David Maurer is a Director in the U.S. Government Accountability Office's (GAO) Homeland Security and Justice team, where he leads GAO's work reviewing DHS and DOJ management issues. His recent work includes reports and testimonies on DHS research and development, DOJ grant programs, the federal prison system, federal judgeships, DHS morale, and DHS's overseas presence.

From 2008-9, Mr. Maurer worked as an Acting Director in GAO's Natural Resource and Environment team, where he managed work assessing U.S. global nuclear detection programs, and enforcement of federal environmental law. Mr. Maurer was also detailed to the House Committee on Appropriations, Surveys and Investigations staff. From 1993-2007, Mr. Maurer managed and led work in GAO's International Affairs and Trade team, where he reviewed U.S. efforts to combat international terrorism and proliferation of weapons of mass destruction, U.S. assistance to the former Soviet Union, peacekeeping in the Balkans, and several other international issues. He also served as the team's manager for staffing and human capital issues. Mr. Maurer began his GAO career in 1990 in GAO's Detroit Regional Office, where he worked on military and environmental issues. In recognition of his contributions to audit work, training, and operational responsibilities, Mr. Maurer has received several GAO awards during his career.

From August 2005 through June 2006, Mr. Maurer was a student at the National Defense University where he was recognized as a Distinguished Graduate of the Industrial College of the Armed Forces and received an M.S. in national resource strategy. Mr. Maurer also has an M.P.P in international public policy from the University of Michigan and a B.A. in international relations from Michigan State University.

(Note: Last name rhymes with "tower").

Chairman BUCSHON. Thank you very much.

I now recognize Dr. Eyerman for five minutes for his testimony.

TESTIMONY OF DR. JOSEPH D. EYERMAN, DIRECTOR, HEALTH SECURITY PROGRAM, RTI INTERNATIONAL; DIRECTOR FOR RESEARCH AND MANAGEMENT, INSTITUTE FOR HOMELAND SECURITY SOLUTIONS, DUKE UNIVERSITY

Dr. EYERMAN. Good morning, Chairman Bucshon, Chairman Broun, Chairman Smith, Ranking Member Lipinski and Ranking Member Maffei, and distinguished Members of the Committee. I thank you for the opportunity to testify today regarding technology needed to secure America's borders. I have prepared written testimony, and request that it be entered into the record.

I have been working closely with DHS Science and Technology Directorate on a series of program and technology evaluations for the past six years in my role as Director of the Institute for Homeland Security Solutions at RTI International. Our work with DHS is part of a larger RTI Project to better understand the human factors that contribute to the transition of new technologies into the public sector and the private market.

I am a social scientist by training, and in my role with IHSS, I have had the opportunity to apply social science research methods to the evaluation of DHS programs and the application of new technologies. In my expert opinion, social science can help us understand the general public, that is, the customers, and the DHS staff who will use the new technologies. This is just as important when developing technologies for securing our borders as it is for the next big project from Apple or Google. Failure to understand the customer can cause us to develop new technologies that are never adopted or never used to their full potential. This increases cost and delays the transition to application.

In our work with the DHS, we use social science methods to support technology development by S&T programs to better understand the end users and customers and things like staffing and training requirements, usability of the new technology, and public perceptions about privacy and safety. As part of our work, we have been fortunate enough to employ these methods in support of several DHS technologies including a DHS S&T-funded assessment of the rapid DNA pilot test, part of a study to develop technology for field DNA tests to support applications by refugees for entrance into the United States; a DHS S&T-funded examination of non-technical barriers encountered by program managers designed to identify trends and patterns that can guide the program managers in the transition of future technologies; and finally, an assessment of non-technical factors that will contribute to the safe and successful transition of unmanned aircraft into the routine aspects of our economic and social lives.

Some of the key findings of these studies that are relevant to the transition of DHS technology to border security are, first, strong and potentially beneficial technologies can be derailed by non-technical problems stemming from a failure to understand the needs and abilities of the workforce, the complexities of public perceptions

and the willingness of the public to accept certain types of technologies into their daily lives. Second, the social science evaluation model is rarely applied to new technologies by DHS, and when it is applied, it is used in a limited and non-standard manner. This may delay the transition of technologies and may limit our ability to assess the impact and effectiveness of those technologies on the agency missions. Finally, complex technologies can develop at a slower rate than the operational realities of the components. This often results in technologies that are developed without a clear operational partner for implementation because needs have changed and priorities have shifted.

My written testimony includes more detail on these and other technology assessments. We continue to examine these challenges and make recommendations for changes that will expedite the transition process to bring new technologies to bear on our security needs in a more efficient and timely manner.

Thank you for your interest, and thank you for any questions you may have.

[The prepared statement of Dr. Eyerman follows:]

U.S. House of Representatives
Committee on Science, Space, and Technology
Subcommittees on Research and Technology and Oversight
Technology Needed to Secure America's Border

Written Testimony

Dr. Joe Eyerman
Director, Institute for Homeland Security Solutions
RTI International
July 31, 2014

Good morning Chairman Bucshon, Chairman Broun, Ranking Member Lipinski, Ranking Member Maffei, and distinguished members of the Committee. I thank you for this opportunity to testify today regarding the *Technology Needed to Secure America's Borders.*

The successful use of technology to secure our borders depends on the ability of staff within Customs and Border Protection and Immigration and Customs Enforcement to employ the technology in a meaningful way that allows them to more effectively or efficiently engage the public they serve. Our social and behavioral research on private and public sector technology development demonstrates the critical importance of engaging the customer early and often in the research and development (R&D) cycle. Successful engagement facilitates the transition from R&D to application or consumption. Failure to engage the customer can result in orphaned technologies that are fully functional but are never fully exploited. Valuable and relevant technologies more often than not fail to leave the lab or fail to realize their full potential because they are not properly tailored to the needs of the customers.

Background

I have been working closely with the Department of Homeland Security Science and Technology Directorate (DHS S&T) on a series of needs assessments, requirement analyses, and program and technology evaluations for the past 6 years in my role as Director of the Institute for Homeland Security Solutions (IHSS). IHSS is a consortium that includes Duke University, University of North Carolina, and the nonprofit RTI International. Our work with DHS S&T is part of a larger effort to apply the theories and methods developed in the social and behavioral sciences to examine the effectiveness of programs and new technologies for advancing the specific missions of government agencies. Our work includes qualitative and quantitative assessments of programs and technologies and draws on the evaluation techniques used at RTI and other research organizations to assess programs throughout the federal government.

In addition to my work with DHS, I have also taught social science research methods to graduate students in the United States and Ireland. I have also worked closely with several private sector technology development and assessment programs. In these roles, I have come to appreciate the

value that strong social science research methods can add to technology development in the private, academic, and public sectors. Specifically, these methods allow us to better understand the needs of the customers who will use the technology in their jobs and daily lives. This understanding can accelerate the technology transition process and bring more effective and efficient technical solutions to meet our nation's border security needs.

Role of Social Science in Security Programs and Technologies

Social science methods have been used extensively to support private and public sector technology development. The social and behavioral sciences are designed to study the interactions of individuals and groups in a variety of settings and generally include the fields of economics, sociology, psychology, political science, communications, anthropology, criminology, and related disciplines. The standard methods used in modern social science include a suite of quantitative and qualitative data collection and analysis techniques that are designed to assess explanations of the social world with data that measure human behavior. These techniques are often used to assess the current state of group knowledge, attitudes, and beliefs; change in group composition and behavior over time; and the impact of social change on current group dynamics. These same methods and techniques are particularly valuable for assessing the effectiveness of governmental policies because they allow us to measure change in the condition of groups and individuals resulting from social interventions such as new programs and technologies.

Our application of the social science method has been to examine the impact of programs or technologies on the community of practice and the community of benefit. The community of practice includes all of the people who will use the technology in support of their role in achieving the agency mission. For example, in our work with the Transportation Security Administration (TSA) we examined the use of x-ray technologies with Transportation Security Officers, trainers, managers, and key decision makers. The community of benefit includes all of the members of the general public who are exposed to policy or technology in its application for the agency mission. In the TSA example, the community of benefit includes any member of the public who travels through TSA-managed airports. Both communities must be examined to fully understand the presence and nature of the need for the technology, the impact of the technology on the agency mission, and possible barriers to a successful transition of the technology or program to operational use.

IHSS has been conducting a series of program and technology evaluations for DHS S&T since 2008. Some examples of these evaluations are the following:

- **Rapid DNA Testing.** A DHS S&T–funded project to evaluate the integration of low-cost, rapid DNA screening technology into the programmatic activities of United States Citizenship and Immigration Services (USCIS) criminal checks and kinship verifications. Our research includes an assessment of the ability of USCIS workers to

engage the technology in their work processes and an assessment of the acceptability of the technology to applicants in refugee camps.

- **Technology Acceptance Evaluation.** A DHS S&T–funded project to examine the *nontechnical* barriers to successful transition of new technologies from the laboratory to the operational setting in the DHS components. This project assesses the potential barriers related to privacy, policy, organizational structures and practices, staff perceptions and capabilities, and public perceptions. By working with teams of private sector technology developers, government R&D program managers, and the general public, we will produce a set of best practices to guide the transition of new technologies into the DHS operational environment.
- **TSA Personnel Evaluation.** This DHS S&T project enhances the TSA Office of Security Operations' existing Officer Performance Studies project by expanding the evaluation of search capabilities for TSA. This will be done by developing new visual search techniques to assist with the review of x-ray images combined with an assessment of the working conditions, job requirements, training process, and performance measures of TSA workers. This study uses research methods from cognitive psychology to measure the visual searching processes employed by TSA workers to develop new training methods and technologies.
- **Unmanned Aircraft Systems (UAS) and the Human Element.** An internally funded project to assess the nontechnical factors that will contribute to the safe and successful transition of UAS into the routine aspects of our economic and social lives. This project examines the UAS technology transition into the communities of practice and benefit using public opinion data, assessments by law enforcement officers, and a comparative analysis to other technologies.

Current Coordination Between DHS Technology Development and Communities of Practice and Benefit

Overall, DHS does not draw extensively on the social and behavioral sciences to assess the impact of its programs and technologies on the agency missions and the populations served. In some cases, such as those listed above and the work carried out by some of the DHS Centers of Excellence and by other contractors, DHS has embraced social research to advance its understanding of critical security issues, its workforce needs, and the populations served. However, the number of DHS staff assigned and the frequency of the application of the standard social and behavioral evaluation model for DHS-funded programs and technologies is very limited and lags behind the more robust and prevalent evaluation procedures employed by other Departments in the federal government. This is in part a result of the pressure immediately following the establishment of the Department to develop quick solutions to keep our nation secure across a very large mission space. However, now that DHS is well into its second decade, the establishment of standard impact evaluation requirements for new technologies and programs on the human aspects of the agency should be possible and expected. DHS should establish a

social and behavioral sciences unit within S&T and task it with coordinating evaluations of the impact of new technologies and programs throughout the components on its specific mission, its workers, and the populations it serves. Such a unit would result in more timely, effective, and efficient technology transfer that promotes a secure homeland.

Furthermore, a dedicated social and behavioral sciences unit within DHS headquarters would promote the coordination between the technology development at S&T and the transition and implementation in the operational components through a standardized evaluation design. Such a design would engage the community of practice in the operational components and the community of benefit at all stages of the technology evaluation, starting with the early needs assessment through workforce and public reactions to the technology and intended uses prior to transition, to the assessment of the effectiveness and acceptability of technology for meeting mission requirements and satisfying public standards of acceptability after implementation. The stages of a good social and behavioral evaluation model should include at least the following:

- an assessment of the operational need in the community of practice that will benefit from the new technology;
- an assessment of the ability of the community of practice to employ the technology, including the identification of gaps in staffing and training that must be addressed before the technology can be transitioned to practice;
- an evaluation of perceived risks, threats, or biases associated with the technology by the community of benefit; and
- an assessment of the technology on the operational mission of the components following the transition and over time.

Key Findings From Our Research

As indicated above, the IHSS team has conducted a series of DHS S&T–sponsored technology and program evaluations using methods from the social and behavioral sciences. Some of the key findings of these studies include the following:

1. Strong and potentially beneficial technologies can be derailed by nontechnical problems stemming from a failure to understand the needs and abilities of the community of practice and the willingness of the community of benefit to accept the technology in their daily lives.
2. The social and behavioral evaluation model is rarely applied to new technologies, and when applied it is used in a limited and nonstandard manner, which reduces its value and prevents comparability of its value to other transitioned technologies.
3. Private sector R&D programs encourage frequent and early engagement of communities of practice and benefit in the design, planning, and implementation of new technologies. Similar procedures will increase the relevance, value, and efficiency of DHS S&T technology development.

4. Complex technologies can develop at a slower rate than operational realities of the components, often resulting in a technology that is less desired and useful than when the original technology transfer agreement was developed between DHS S&T and the operational components.
5. Management priorities and funding levels can shift and change during the R&D cycle, leaving potentially beneficial solutions without sufficient budget or organizational support to implement.
6. Public perceptions of technology can be more complex and dynamic than may be expected by technology developers. As a result, technologies that the public may consider relatively benign and nonthreatening may produce an unexpected backlash when introduced to the community of benefit. In addition, the tolerance of new technologies and the perceived impact on privacy and safety can change over time and significantly affect the ability to use new technologies in an operational context.
7. The assessment of operational requirements, workforce capabilities, and public perceptions can support both the technology development and the communication plan between DHS S&T and the operational components.
8. The DHS S&T technology transfer process is inconsistently applied across programs, rarely draws in all members of the community of practice, and rarely addresses the public perception issues in the community of benefit. This could be resolved through better coordination of the evaluation plan in DHS S&T.
9. Careful assessments of the technical needs and operational abilities of the user communities, and thorough assessment of the effectiveness of new technologies to support agency missions, are both expensive and time consuming. These time and cost requirements can be reduced through standardization and better coordination of the evaluation process.

Conclusions

Successful technology transition requires attention and accommodation of both nontechnical and technical issues. The nontechnical issues can be addressed by applying evaluation techniques from the social and behavioral sciences to assess the needs, abilities, and perceptions of the community of practice in the DHS workforces and the community of benefit in the general public. The application of these techniques is most effective if engaged early in the design phases of technology development and used through development and transition to track the changing mission needs, workforce, and public perceptions. Finally, this same model can be used to assess the effectiveness of DHS programs and technologies by measuring change over time and the impact on the mission requirements.

Joe Eyerman Biography

Dr. Joe Eyerman is the Co-Director of the Institute for Homeland Security Solutions, a senior research methodologist, and the Director of RTI International's Center for Security Safety and Defense. Dr. Eyerman has more than 17 years of professional experience statistically modeling social behavior and managing data collection and analysis projects. His substantive interest is in the formal and statistical modeling of decision processes related to political behavior, terrorism, and radicalization. His recent methodological work has focused on the relationship between the data collection process and error in population estimates on a variety of bioterrorism, public health, and surveillance studies. Dr. Eyerman has conducted methodological studies to investigate ways to improve data quality and studies of survey nonresponse. He is an experienced project manager, survey methodologist, and data analyst. His training is in political science and social science research methods, and he teaches social research and program evaluation methods in the United States and Ireland. He has worked on several private and public sector technology development programs to assess the human aspects of technology development and acceptance. He has worked closely with the Department of Homeland Security for the past 6 years on a wide range of social and behavioral science studies, including evaluation of new technologies and programs, privacy assessments, and public perception panels.

Chairman BUCSHON. Thank you very much. I want to thank the witnesses for their testimony, and at this point remind Members that Committee rules limit questioning to five minutes. The Chair at this point will open the round of questions. I recognize myself for five minutes.

Dr. Riley, what is the feasibility of adopting existing surveillance systems such as those used in Iraq and Afghanistan on the southern border?

Dr. RILEY. It is hard to answer the question without additional information.

Chairman BUCSHON. Well, for example, DoD has surveillance equipment that we currently use in Iraq and Afghanistan, mobile equipment and others that have some potential that we may not need to do duplicative scientific and technical research on that would make them applicable with the dual-use purpose of being used on the southern border, a similar concept.

Dr. RILEY. I would be in favor of a structured test to understand how they would work at the U.S. border and in which ways they can be effective, but at this point I am not convinced that we need significant investment in new technologies more than we need careful assessment of what we already have in place and how well the pieces work together.

Chairman BUCSHON. Understood.

Mr. Maurer, from your past work with S&T, what are the most important lessons learned that you would like—you would share with the new S&T leadership?

Mr. MAURER. Well, I think first and foremost, I would highlight the two remaining outstanding areas they have to show some more progress on, which is namely do a better job tracking and a better job coordinating the R&D efforts, not just within the Science and Technology Directorate but across the entire Department. S&T has had statutory responsibility, and frankly, they have struggled with having a close—having close coordination with some of the other operational components that are doing R&D activities. I would encourage them to take action on that front and ensure that what they—the other thing I would have them do is ensure that they are more tightly in tune with the needs of the eventual end users of the technologies they are developing. They are making strides toward that. His predecessor spent a lot of time and effort trying to get S&T more tightly bound with not just R&D but getting involved in acquisition as well, and I think that is a good step.

Chairman BUCSHON. I would agree with that, that it may very well be important to coordinate with the potential end user, although sometimes the end users don't really know what they might need until the inventors or people invent something that might be useful. I think Apple did that. That was kind of why they did no product research because they felt like people didn't really know what they would use until you develop it. So there is two arguments there, but I do think better coordination is very important.

Through its authorizing statute, DHS S&T is responsible for developing a national policy and strategic plan for the federal government's civilian efforts to identify and develop countermeasures for emerging terrorist threats. S&T is also tasked with coordinating the development and management of science and technology agen-

da for DHS. To the best of my knowledge, DHS S&T has not yet accomplished either of these responsibilities.

Dr. Riley and Mr. Maurer, both of you testified about the lack of coordination for border technology R&D within DHS. As we look toward reauthorizing the S&T Directorate, should these strategic planning and coordination responsibilities remain within DHS S&T? If so, how can we prompt movement on these important tasks? If not, where might they better be situated, and why? Mr. Maurer?

Mr. MAURER. Yeah, I think it is important under the current statutory framework for S&T and the Department to do what the law required them to do, which is establish a strategy for within the Department and work with our partners across government. The broader policy issue of whether they should continue to have that responsibility and others, there is reauthorization language, is really a policy consideration. One thing that is important to keep in mind is that the amount of money that DHS spends on R&D is about one-sixth of the total that is spent across the entire federal government on Homeland Security-related R&D. So somebody somewhere is going to have to be involved in trying to bring coherence and coordination and oversight on that—on those funds.

Chairman BUCSHON. Dr. Riley?

Dr. RILEY. I will just add that one of the things that may or may not help—I am not sure I have made up my mind on this—is better use of Under Secretary of Policy in the Department of Homeland Security. Right now that is an Assistant Secretary position, and one of the ways in which stitches may be dropped between the generation of technology and implementation and effective use of them is perhaps not having a counterpart on policy formulation and execution.

Chairman BUCSHON. Thank you. I recognize Mr. Lipinski for his line of questioning.

Mr. LIPINSKI. Thank you.

Dr. Eyerman, you have been working directly with DHS S&T for the past six years in evaluating their programs. In the latter part of your testimony, you listed a variety of barriers to successful transition of new technologies from the laboratory to the operational setting in the DHS components. Could you elaborate on what DHS can do to further the transfer of technology to users, and do you have any idea what has held DHS back in developing a strategy to address these challenges?

Dr. EYERMAN. Thank you for your question, Mr. Lipinski. I would say there are two issues that have affected the ability to increase the involvement of social science research in DHS technology transition. One is the absence of a standardized process for inserting social science research that involves the end users and the customers and the DHS staff in the study design, the project implementation and the assessment of the results, and I think that is primarily due to a lack of coordination within S&T around the social sciences. At one point there was a division in S&T focused on the human factors. That division has been removed and merged in with another division, and staff have been eliminated.

Mr. LIPINSKI. Was there any particular reason that that was removed that you know of?

Dr. EYERMAN. I don't know the reason behind that. That is beyond my knowledge. I do know that many of the staff were retained but the second barrier, I think, to the adoption is the number of staff that are focused on social science research methods at DHS. I think the first issue could be addressed with better coordination and planning and a standardized process for inserting evaluation of the customers and the workers in the R&D cycle. The second one is more of a staffing and budget issue.

Mr. LIPINSKI. Thank you.

Dr. Riley, you mentioned in your testimony that after many years, we are still lacking the analytic capability to measure the effectiveness of our border security tools and policy mechanisms. I understand your solution for measuring this is further investment in developing a strategy for R&D and investment in technology infrastructure. Considering there are various types of illegal border activity with no one-size-fits-all solution, what types of technologies should we invest in to get the necessary data and models?

Dr. RILEY. Well, in terms of technology development and investment in that area, I think one of the things I would be looking for is a tighter and better designed requirements generation process so that we understand where the frontline providers of border security feel the need for new technologies and perceive the need for additional technology development. There has been some progress made in that area but generally, for example, the connection between technology transfer and requirements development in DHS is not as mature as it is, say, in the Department of Defense.

Mr. LIPINSKI. What is the reason for that? Just, it has not been developed?

Dr. RILEY. I think growing pains, and there are significant structural differences between the Department of Defense and the Department of Homeland Security but I think the mere process of trying to incorporate all of the different elements that went into DHS and get them functioning smoothly is probably a limiting factor.

Mr. LIPINSKI. Okay. And Mr. Maurer, according to multiple GAO reports, DHS is missing a strategic plan, which we had talked about. Further, it can't track its investments in R&D and thus cannot identify the total investment it has made in R&D. GAO has made recommendations to solve these problems but DHS has been quite vague, saying that it has taken some steps to update guidance. Since your office has been monitoring their progress, do you have an idea as to what has been getting in the way of developing this plan?

Mr. MAURER. That is a really good question because we have been recommending—some of this goes back to a report that was issued two years ago, so DHS would be better placed to give the specific reasons. Our sense is that they certainly made progress on defining R&D, so that is the first step, but we would like to see them develop a strategy for the whole Department. We would like to see them develop a way to clearly articulate what processes and coordination mechanisms need to be in place, have a more effective way of implementing the various R&D projects across the Department. I would hope that the relatively new Under Secretary would take this on as one of his top priorities in his new role.

Mr. LIPINSKI. Thank you. That—I yield back.

Chairman BUCSHON. Thank you, and I now recognize Chairman Broun for five minutes.

Chairman BROUN. Thank you, Mr. Chairman. I want to follow up on a question. In my opening statement, I mentioned that DHS needs a technology roadmap to manage its R&D activities. What is DHS's biggest impediment to developing that organized and comprehensive national border security strategy? I will start with Mr. Maurer.

Mr. MAURER. I would say that probably the biggest challenge they face is just the sheer complexity of the task that they are trying to accomplish. It involves predominantly at CBP but it is going to involve Science and Technology and other parts of the Department as well. It is a multifaceted problem, which touches on many different aspects of the Department, so it is a difficult challenge that they face, and trying to come up with a comprehensive strategy is also difficult. Now, we have been somewhat critical of the Department on different aspects of border security and their ability to measure the impact of the technology investments, for example, that they have made over the past many years. If they can make progress on that front, that would help get them further down the road where they need to be on developing a comprehensive strategy for border security.

Chairman BROUN. Well, if you can give us part of what we call QFR, questions for the record, recommendations of how to get over this impediment.

Dr. Riley, do you have any comments on this also?

Dr. RILEY. Just jotting a note to myself. The border is obviously a complex issue. Different pieces of bureaucracy even within the Department of Homeland Security touch on the border, and nobody really owns it. We need to find a way to get a greater single point of accountability on the breadth of border issues, whether that is something that is, as I said in previous comment, integrated in an Under Secretary for Policy, whether it is the appointment of a border czar as we have done on other policy issues in other contexts. I am not quite sure. But there is no single point of accountability on the border, and having that may be something that prompts progress.

Chairman BROUN. Mr. Maurer, let me read to you a few sentences from your own testimony related to DHS R&D activities. You said, "S&T officials told us at the time that a process did not exist at DHS or within S&T to prevent overlap or unnecessary duplication. We also found in September 2012 that neither DHS nor S&T tracked all ongoing R&D projects across the Department including R&D activities contracted through the National Laboratories. As part of our review, we identified 11 components that reimbursed the National Laboratories for R&D from fiscal years 2010 through 2012, but S&T's Office of National Laboratories could not provide us with any information on those activities and told us it did not track them. As of July 2014, DHS has not developed new policy guidance."

These are issues going back for a couple of years. Now, I understand that in some areas, DHS appears to be taking initial steps to meet GAO's multiple recommendations such as conducting portfolio reviews across the Department and collecting feedback from

customers, but this Department is no longer in its infancy. In fact, it has been around for over a decade now, and when I read that DHS has not yet determined the most effective path to guide R&D across the Department or that S&T has not developed new policy guidance, I have to ask, should some or all of DHS's R&D components be placed on GAO's high-risk list, which, as you know, is reserved for agencies in program areas vulnerable to fraud, waste, abuse and mismanagement, or are they in most need of transformation? So should they be on the high-risk list?

Mr. MAURER. Well, to some extent, they already are. We have an existing high-risk area for——

Chairman BROUN. But have you named them on the high-risk list?

Mr. MAURER. Specifically to R&D?

Chairman BROUN. Yes.

Mr. MAURER. We don't have a specific shout-out to R&D but the problems that they face in terms of coordination and tracking are rooted in more fundamental issues with the Department's inability to stitch itself together in a comprehensive way, so we have a high-risk area for management at DHS, which has been critical of DHS's efforts to develop a common approach to acquisition and financial management, information technology, human capital. A lot of these things are the building blocks of organizations, and to some extent are some of the root causes as to why DHS doesn't have visibility over R&D spending. They don't have the financial systems that allow them to do that, for example.

Chairman BROUN. Well, my time is about up. I encourage you to put them on the high-risk list because just by your own testimony, there is just tremendous problems there, and I think they should be and I encourage you to do so.

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

Chairman BUCSHON. Thank you. Votes have been called but we do have some time, so we are going to go ahead—I am going to go ahead and recognize Mr. Maffei for his line of questioning, and then we will see where we are and then go from there.

Mr. MAFFEI. Thank you, Mr. Chairman.

Mr. Maurer, first of all, I apologize for giving you a doctorate in my opening statement. You can pick that up after the hearing.

I really appreciate the work of all the witnesses on this, and it has been a very informative hearing.

One thing I want to ask you, Mr. Maurer, is, DHS has had some rather large R&D failures. One example is that they canceled a very large and one of the most comprehensive technological investments, SBInet, after investing nearly a billion dollars. Has this changed at all the way they are approaching it, and are they able to salvage any of that technology?

Mr. MAURER. You are absolutely right. SBInet was a failed project at DHS. DHS has a slightly different approach to developing new technology for the border. They have the Arizona Technology Plan. DHS's current approach is to rely more extensively on commercial off-the-shelf technology and using that to deploy for security—for helping secure the border. We still have some concerns about how that particular program is being implemented, specifically in the area of testing. We have issued reports and we have

testified previously that we don't believe that the amount of testing that is going to be done for the Arizona Technology Plan is sufficient. That was one of the root causes of the problems that plagued SBInet, so our hope is that DHS will take us up and adopt our recommendation.

Mr. MAFFEI. Thank you.

Dr. Riley, can you give me any sense, how robust is this technology? I don't want to be cynical but sometimes you get the impression that—I mean, I have got a bunch of friends from high school who are really good technically and they could come up, set up motion sensors, cameras, lasers, even UAVs now, and for much a cheaper cost do a lot of the same thing. Tell me I am wrong.

Dr. RILEY. The technologies are good and mature. I think one of the areas where DHS and, frankly, many government agencies struggle is kind of the tooth to tail, where do you have the people to back up and integrate with the technology to make the most and best effective use of it. DHS is making progress in this area. Their acquisition processes are maturing, but they are certainly not perfect at this point.

Mr. MAFFEI. Thanks.

Dr. Eyerman, do you have anything to add, particularly involving that human—the human element there?

Dr. EYERMAN. Absolutely. I completely agree with Dr. Riley's comments. We worked on an evaluation of a technology for biometric identification at the airports. The technology was quite ready. It was off the shelf. It was effective. The problem was, is the technology couldn't be integrated into the human systems, and that is where it would break down, because if it was integrated into the human systems, it would result in large delays at the airport. It was unclear who would be responsible for implementing the technology, and there were serious cost implications for the airlines which couldn't be addressed by the technology, only by research into the humans.

Mr. MAFFEI. Thank you very much. I am going to yield my final two minutes to the gentlewoman from Connecticut, Ms. Esty.

Ms. ESTY. Thank you.

A quick question, a follow-up for you, Mr. Maurer. You had mentioned that only a sixth of the R&D funding around border issues is actually done with DHS. We have already heard considerable testimony how that isn't even managed very well. So where is the other five-sixths? Who are the lead agencies and how should we be thinking about who sets the strategic goals, how can they be better coordinated? I would really like your advice, and then if others want to chime in. Thank you.

Mr. MAURER. Sure. Absolutely. DHS is one-sixth of the total pie for all of Homeland Security R&D, so we don't know how it breaks out specifically for border, but the other five-sixths for all Homeland Security, a lot of it is being done at DoD and the Department of Health and Human Services. Writ large one thing that would help that overall coordination is the development of the statutorily required, government-wide approach to Homeland Security R&D, and that is something that has been on the books for a number of years.

Ms. ESTY. Thank you. Anybody else?

Dr. RILEY. I will just say that I think in conversations and discussion about the border, it is common to lapse into thinking only about the southern land border and we really need to be more careful thinking holistically about air, sea and land borders north and south.

Ms. ESTY. Coming from Connecticut, we think about this in terms of our ports, and it is an issue. We have the Strategic Petroleum Reserve in my state. We have nuclear plants all up and down the East Coast that are right on the coast, and I heartily agree. We can't just be thinking about the southern border. Thank you.

Chairman BUCSHON. I now yield to the Chairman of the full Committee, Mr. Smith.

Chairman SMITH. Thank you, Mr. Chairman.

First of all, I would like to enter into the record two items from Petro Data Communications.

Chairman BUCSHON. No objections. So ordered.

Chairman SMITH. Thank you.

[The information appears in Appendix I]

Chairman SMITH. And let me say to our witnesses, we are going to try to squeeze in two more questions in the next 7 or 8 minutes, so if you could give brief responses to my questions, we will see if that works.

Dr. Riley, let me address my first question to you, and that is, in 2011, the Administration canceled a Secure Border Initiative. In 2012, it withdrew 1,200 National Guard troops from the border. Do you think the result of those actions made it easier for illegal immigrants to cross the border?

Dr. RILEY. It is difficult to say, Mr. Chairman, but both of those were important initiatives that I frankly would like to see followed through on in the near future.

Chairman SMITH. Okay. Thank you.

My next question is to all three of you all, if you would, and that is, how would you grade the Department of Homeland Security on its use of technology today to secure the border? Real quickly, Dr. Riley?

Dr. RILEY. Incomplete.

Chairman SMITH. Dr. Maurer?

Mr. MAURER. I would say the same thing, incomplete.

Chairman SMITH. Okay. And Dr. Eyerman?

Dr. EYERMAN. I agree.

Chairman SMITH. Okay. What type of technology are they using, Dr. Riley or Dr. Maurer?

Mr. MAURER. There is a large range of technologies from unmanned aerial stats and——

Chairman SMITH. You are saying just a lot more they could be doing? Is that what you meant by "incomplete"?

Dr. RILEY. It is simply too complicated an issue to grade out in a few minutes before a Committee like this, I think.

Chairman SMITH. Okay. Well, we will take the "incomplete" for the time being.

Mr. Maurer, I want to ask you a question about the GAO. In 2011, you took a look at, I think, 873 miles of border and you said only 15 percent was under control of the Border Patrol. What did you mean by "under control"? How would you define that?

Mr. MAURER. In that report, we were using a measure that CBP used at that time for operational control of the border. CBP no longer uses that particular measure in their effort to assess border security.

Chairman SMITH. But my question was, what did the definition mean when you undertook this study of control of the border only 15 percent?

Mr. MAURER. I think that was part of the problem, and that is part of the reason why CBP moved away from that definition. It was open to a wide interpretation.

Chairman SMITH. I think the reason they moved away because it was embarrassing that only 15 percent of the border was under full control, myself, but again, full control, I was told in a previous hearing, meant that there was a high likelihood that illegal immigrants would be intercepted.

Mr. MAURER. That is correct. That tracks back to the work that we did in 2011.

Chairman SMITH. Okay. Which led to 85 percent of the border under something less than full control.

Thank you, Mr. Chairman. I am going to yield now the remainder of my time to the gentleman from Arizona, Mr. Schweikert.

Chairman BUCSHON. I ask unanimous consent to allow Mr. Schweikert to participate in the hearing. Without objection, the Chair then— it is ordered.

Mr. SCHWEIKERT. You mean I could have objected to myself being here?

Okay. Let us see if we can do a quick lightning round here. Dr. Riley, in your written testimony, and I think actually in your spoken testimony, there was a comment about some of the access to data and how much data was sort of off the books or you were not allowed to gain access to. Can you give me a quick snippet of how that affects trying to create policy and design?

Dr. RILEY. It limits the ability to interact in the academic and analytic communities, and it has a stifling effect on being able to develop innovative approaches to border security.

Mr. SCHWEIKERT. So if Dr. Eyerman is trying to look at data sets to build human interaction, he doesn't actually have enough robust data sets to work from?

Dr. RILEY. It is not only the availability of the data, although that is certainly the case. Those data need to be collected and the data sets built, but it is also the ability to draw on our academic partners. IHSS has a consortium with Duke and UNC, and many of the universities won't work on data that is not publishable.

Mr. SCHWEIKERT. Well, and formerly Dr. Mr. Maurer, you actually almost just touched on this, that for many of us who are trying to get our heads around border policy, being from a border state, the definitions keep changing on me. One day we calculate it this way, the next day we calculate it this way. One day, for human smuggling, you know, if you are captured in this distance, you are considered deportation. The next day that is redefined. When you are doing your analysis, is this a continued problem of constantly moving the definitions, let alone the access to the actual data for the researchers?

Mr. MAURER. That certainly makes it more difficult to have a consistent—they don't have consistent measures for assessing border security, and they change from year to year going back to 2011, so that does make that more challenging. And we have had reports that have talked about the important need for that, most critically having a need to assess the impact of the technologies that have been deployed on the border. We have been critical of CBP's inability to demonstrate the extent to which deployed technology, what impact it has security.

Mr. SCHWEIKERT. Mr. Chairman, I know I am over time but from my understanding, this is actually a bigger issue than a lot of people understand. It is hard to know what you are chasing when two things happen: they don't tell you or they change that definition. And then there's the whole more cultural decision of can you ever have a large bureaucracy be as nimble and flexible when trying to design fixed technologies when the other side is incentivized to constantly beat that technology and be more nimble for the profit side. Thank you, Mr. Chairman.

Chairman BUCSHON. Thank you.

At this point I would like to thank the witnesses for their valuable testimony. We will not be returning after votes. We will be adjourning here shortly as everyone has been able to ask their questions. Your written testimony and your oral testimony is very valuable to the Subcommittee. Members of the Committee may have additional questions for you, and we will ask that you respond to those in writing. The record will remain open for two weeks for additional comments and written questions from Members.

At this point the witnesses are excused and the hearing is adjourned.

[Whereupon, at 11:06 a.m., the Subcommittees were adjourned.]

Appendix I

Answers to Post-Hearing Questions

ANSWERS TO POST-HEARING QUESTIONS

Responses by Dr. K. Jack Riley

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY
SUBCOMMITTEE ON OVERSIGHT

"Technology Needed to Secure America's Border"

Dr. K. Jack Riley, Vice President, RAND National Security Research Division, Director, RAND National Defense Research Institute

Questions submitted by Rep. Larry Bucshon, Chairman, Subcommittee on Research and Technology and Rep. Paul Broun, Chairman, Subcommittee on Oversight

1. What would it take to fully integrate the federal, state and local border security technologies and information in a way that better supports future R&D efforts?

   Response:
   Border security technologies and information should be integrated into a model or simulation of the border. I think of this modeling effort as something analogous to the war gaming, scenario development, and simulation conducted by the Department of Defense. These simulation efforts are useful for a variety of reasons, including understanding information gaps; combining technologies to pursue policy goals; identifying technology gaps; and exploring how changes in one component or segment of a border may affect other components.

   This simulation tool could be created and maintained for relatively modest federal investment. Based on experience in other policy realms, I estimate that an initial investment of less than $10 million, and an annual investment of approximately $1.5 million, would be sufficient. That is a relatively small price considering the billions spent on border security.

2. Is DHS S&T taking advantage of what private industry can offer in R&D to fully integrate the different border security technologies? Has DHS S&T asked private industry to support their R&D efforts for securing the southern and northern borders?

   Response:
   DHS S&T is not taking advantage of what the private sector can offer in one sense: it has not procured assistance to develop an integrated model of the border. There are many firms (including, full disclosure, my own employer, the RAND Corporation) that are free of conflicts of interest and capable of doing this.

   With respect to actual security technologies themselves, I am not in a position to assess the sufficiency of DHS.'s outreach to the private sector. There appears to be no shortage of technology vendors in this area. However, we do not have the ability to judge the effectiveness of their technologies because we lack a framework for assessing their cost-effectiveness.

3. Does the U.S. have adequate and effective border security given the current technology in place? What are your biggest concerns about the current technology being implemented at the border? Do you believe there is a way to remedy these problems in a timely fashion? Can you tell us how much of the border is under persistent surveillance at any given moment? How is effectiveness measured? What should our ideal goal be in terms of effectiveness in order to appropriately protect American citizens? What kind of R&D and technology would you want to see utilized in an effective national border control strategy?

Response:
In an ideal policy-making world, we would have information .– or a tool .– that guides us on how to combine policies and technologies to achieve optimal effects. The fact that we do not have such a tool is, in my estimation, the single largest security gap at the border. Unless or until we invest in understanding the effectiveness of our technologies and policies, we are potentially throwing away taxpayer resources.

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY
SUBCOMMITTEE ON OVERSIGHT

"Technology Needed to Secure America's Border"

Dr. K. Jack Riley, Vice President, RAND National Security Research Division, Director, RAND National Defense Research Institute

Questions submitted by Rep. Scott Peters, Member, Subcommittee on Research and Technology

1. Regarding embassy perimeter security, a senior policy expert from RAND testified in 2012 about long-range communications technology, also called acoustic hailing devices, that can provide a non-lethal capability when used at very high volumes without causing any permanent harm. This communications and access denial technology is being used by the Army in Afghanistan, on ships by the Navy, and by police forces all over the world. What is the potential utility of such technology on the border? Has CBP reviewed or tested acoustic hailing devices in terms of their potential application on the border and if not, are you aware of a specific reason?

   Response:
   Like many technologies, acoustic hailing has the potential to contribute to border security. However, we cannot say whether acoustic hailing would be more or less effective than other technologies; whether it would best be paired with other technologies or deployed stand-alone; or how much acoustic hailing capacity we would need. We cannot answer these questions because we do not have effective models or simulations available that help us understand the technology and policy tradeoffs at the border.

   I do not know if CBP has tested this technology. If the technology has been tested, it would benefit the scientific community and the border security planning and policy communities to make the analysis publicly available.

Responses by Mr. David C. Maurer

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY
SUBCOMMITTEE ON OVERSIGHT

"Technology Needed to Secure America's Border"

Mr. David C. Maurer, Director, Homeland Security and Justice, U.S. Government Accountability Office

Questions submitted by Rep. Larry Bucshon, Chairman, Subcommittee on Research and Technology and Rep. Paul Broun, Chairman, Subcommittee on Oversight

1. At our hearing in July, you were asked what DHS's biggest impediment was to developing an organized and comprehensive national border security strategy. You spoke of how DHS is faced with a complex task and runs into challenges with working alongside multiple invested parties. You also mentioned that GAO has been critical of DHS's ability to measure the impact of technology investments that they have made over the years, and if progress was made on that front, they would be closer to developing a comprehensive strategy for border security. Do you have any specific recommendations or suggestions on how DHS can move past these hurdles and achieve the ultimate goal of an efficient technology roadmap to manage DHS's R&D activities?

Response:

DHS could better manage and leverage its R&D activities by implementing the recommendations we made on its acquisitions management and those specific to its R&D efforts. We have previously reported DHS has faced challenges testing and acquiring technologies to ensure that they work as intended in their operational environment. In addition, our work at DHS has found that the department has made progress strengthening its management functions, including developing policies that provide a framework for addressing management challenges. However, we have found in our past work that DHS does not always adhere to its own policies. For example, DHS's acquisition policy largely reflects key acquisition management practices, but in September 2012, we found that the department has not implemented the practices consistently. Further, we found that DHS has made progress in initiating efforts to validate required acquisition documents.1 However, the department did not have the acquisition management tools in place to consistently demonstrate whether its major acquisition programs are on track to achieve their cost, schedule, and capability goals.

As we reported in 2012, the challenges that DHS has historically faced related to acquisition is similar to the challenges DHS faces in managing its R&D efforts. 2 Further, we reported that DHS officials told us that there is no distinct line between capital investments and the R&D for technology development. For example, National Protection and Programs Directorate (NPPD) officials told us they consider its cybersecurity system to be a capital investment, and not R&D, but they consider R&D of new technologies as an important aspect of this system. The variation in R&D definitions may contribute to the unreliability of the reporting mechanisms for R&D investments in budget development and execution.

Strengthening its management of acquisition would also help ensure that the technologies that feed into the acquisition process meet mission needs.

Additionally, we recommended in September 2012 that DHS develop policies and guidance for defining, reporting, and coordinating R&D activities across the department, and establish a mechanism to track R&D projects. DHS concurred with the recommendation and, as of September 2014, had updated its guidance to include a definition of R&D but efforts to develop a process for coordinating R&D with other offices remain ongoing and have not yet been completed. Further, according to DHS officials, the department implemented a portfolio review process, as directed by committee reports accompanying the fiscal year 2013 DHS appropriations act, which is aimed at better coordinating R&D activities.3
With respect to border and maritime R&D activities, S&T reported in July 2014 that it was developing three border and maritime related technology roadmaps that will guide its R&D efforts in that area. Specifically, these technology roadmaps focus on (1) land border security, (2) cargo security, and (3) maritime border security. We believe that if appropriately executed and prioritized by component partners, these efforts may help ensure that the technologies that DHS develops or acquires helps components achieve their respective missions.

1GAO, *Homeland Security: DHS Requires More Disciplined Investment Management to Help Meet Mission Needs,* GAO-12-833 (Washington, D.C.: Sept. 18, 2012).

2GAO, *Department of Homeland Security: Oversight and Coordination of Research and Development Should Be Strengthened,* GAO-12-837 (Washington, D.C.: Sept.12, 2012).

3H.R. Rep. No. 112-492, at 133; S. Rep. No. 112-169, at 15-16.

2. Is DHS able to explain specifically how they use their funding for S&T? Does DHS's S&T Directorate break down its budget by project? In general, how transparent and accountable is the DHS S&T Directorate?

Response:

DHS's annual congressional budget justification provides a breakdown of S&T's R&D investments by Program Project and Activity (PPA). The four R&D PPAs in S&T's 2015 budget justification are: (1) Acquisition and Operations Support; (2) Laboratory Facilities; (3) Research, Development, and Innovation; and (4) University Programs. S&T's 2015 budget justification includes a project's description, along with past, current, and planned efforts and requested project costs. For example, under S&T's Land Border Security Area, S&T lists five projects and their costs: 1) Air Based Technologies, 2) Ground Based Technologies, 3) Rapid Response Prototyping, 4) Small Dark Aircrafts, and 5) Tunnel Detection and Surveillance. However each of these projects can comprise several deliverables or sub-projects, and those specific costs are not listed in S&T's 2015 budget justification request.

As we reported in September 2012, within S&T it is difficult to identify all R&D funding because their R&D budget accounts fund both R&D and non-R&D investments. For fiscal year 2011, we estimated that 78 percent of S&T's Research, Development, Acquisition, & Operations account fund R&D activities. DHS has efforts underway to provide more

transparency and accountability for its R&D budget. In response to our recommendation that DHS develop and implement a mechanism to track existing R&D projects and their associated costs across the department, among other things, S&T issued a DHS R&D definition in April, 2014 and is working with the DHS Chief Financial Officer to incorporate the R&D definition into a common appropriation structure. In addition, DHS plans to develop a common appropriation structure for the President's fiscal year 2017 budget request to track all R&D within DHS.

3. Your testimony addressed issues relative to discontinued DHS projects. According to your 2013 GAO report, "DHS's Office of University program officials stated that they expect to routinely discontinue projects that are not demonstrably innovative, progressing, or have no identifiable end user."[1] Why doesn't DHS have better safeguards in place to stop this office from engaging in these demonstrably non-innovative programs in the first place? While your report identifies 19 project deliverables that were discontinued by the Office of University Programs for Centers of Excellence, the amount expended for discontinued R&D is unknown. Why was GAO unable to identify the amount expended for the 19 discontinued project deliverables?

Response:

In our 2013 report, we found that there were a variety of reasons that projects were discontinued.4 It is important to note that the discontinuation of a project or deliverable did not necessarily mean that it was a failed R&D project. In some cases, the R&D results demonstrated that there was no technologically feasible option to address a problem or that a certain type of technology would not provide the desired solution. Further, according to Office of University Programs (OUP) officials, project discontinuation is a good outcome in many circumstances where research success cannot be foretold. These officials added that it is a necessary part of a portfolio-based research strategy.

According to OUP officials, there are several possible reasons why funding for a project is discontinued. Reasons include not making enough progress, the university is not doing the necessary networking with DHS Headquarters to ensure a successful transition, research priorities shift, customer needs shift, or the university began funding research that was not initially agreed to in the cooperative agreement. For example, OUP cancelled a University of Hawaii project on port resiliency because the university's proposed project was not likely to result in a useable deliverable. However, until the university made several attempts to gather a wide range of public and private port security stakeholders the potential outcomes were unknown.

In our 2013 report, we were unable to obtain project level expenditure amounts for the 19 discontinued project deliverables, because the information was not readily available by project at the time of our report, and OUP officials could not confirm the accuracy of the amounts reported for discontinued projects. In September 2014, OUP officials provided GAO with the amounts as reported by the COEs on the 19 discontinued projects, but noted that the cost information had several important limitations. For example, according to OUP

[1] http://www.gao.gov/assets/660/658112.pdf - p.12

officials, the COE Annual Performance reports, which contain some expenditure amounts for some of the discontinued projects, are self-reported by the COEs, and without conducting an audit, OUP cannot confirm they are accurate. In addition, for some of the projects, the figures reported are at an aggregated level (bundled with other projects) and OUP was not able to provide a breakout by project.

[4]GAO, *Department of Homeland Security: Opportunities Exist to Better Evaluate and Coordinate Border and Maritime Research and Development,* GAO-13-732 (Washington, D.C.: Sept. 25, 2013).

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY
SUBCOMMITTEE ON OVERSIGHT

"Technology Needed to Secure America's Border"

Mr. David C. Maurer, Director, Homeland Security and Justice, U.S. Government Accountability Office

Questions submitted by Rep. Randy Hultgren, Member, Subcommittee on Research and Technology

1. In your written testimony, you noted $255 million in R&D from Fiscal Year 2011 that was not reported to OMB as R&D. These were from contracts with industry, universities, and the DOE national labs. Has this issue been resolved, and were all of the contracts with such entities not reported? Also, what was the breakdown in contracts to each sector, and what was the success rate for such research compared to other R&D efforts?

Response:

In September 2012, we reported that DHS did not know how much it spent on R&D activities throughout the department, and that our analysis of data that DHS submitted to the Office of Management and Budget (OMB) found that DHS's R&D obligations were underreported because other DHS components obligated money for R&D contracts that were not reported to OMB as R&D. Specifically, we reported that, for fiscal year 2011, our analysis identified $255 million in obligations for R&D that DHS did not report as R&D contracts in the object classification tables. These obligations included DHS components providing S&T with funding to conduct R&D on their behalf and components obligating funds through contracts directly to industry, universities, or with Department of Energy's (DOE) national laboratories sectors for R&D. Specifically:

• S&T reported receiving $50 million in reimbursements from other DHS components, such as U.S. Citizenship and Immigration Services, the Secret Service, the Office of Health Affairs, Customs and Border Protection (CBP), and the Transportation Security Administration (TSA) to conduct R&D projects.5These obligations were not identified as R&D in these components' budgets.

• Our analysis identified 10 components, including CBP, TSA, U.S. Immigration and Customs Enforcement (ICE), and the Federal Emergency Management Agency (FEMA), that obligated approximately $55 million for R&D contracts that were not reported as R&D. 6

5This figure excludes reimbursements from DNDO and the Coast Guard to S&T.
6We analyzed and identified DHS R&D contracts in FPDS-NG categorized as basic research, applied research and exploratory development, and advanced development.

• Our analysis identified that DHS components, outside of S&T, the Domestic Nuclear Detection Office (DNDO), and the Coast Guard, obligated $151 million to DOE national laboratories for R&D-related projects (44 percent of total DHS spending at the national laboratories in fiscal year 2011). 7For example, NPPD obligated $83 million to DOE national laboratories in fiscal year 2011.

To identify these obligations, we analyzed data from the Federal Procurement Data System Next Generation (FPDS-NG) to identify R&D-related contracts across DHS for fiscal years 2007 through 2011. We filtered these contracts to include only those R&D stages coded as basic research, applied research and exploratory development and advanced development, which align more closely with recognized definitions of R&D. We excluded the other four stages (engineering development, operational systems development, management/support, and commercialization) of R&D because these activities are linked more closely to procurements rather than R&D activities. We also analyzed data from the DOE national laboratories from fiscal years 2010 through 2012 to identify how much DHS components obligated for R&D-related work at the national labs. At the time of our audit, these contracts were on-going; as such we did not analyze the outcomes to determine the success rate for such research compared to other R&D efforts.

To determine the extent to which these issues were resolved, we asked DHS S&T to provide an update on what it was doing to address these findings. DHS S&T officials told us in September 2014 that S&T is working with DHS's Chief Financial Officer to incorporate its R&D definition into a common appropriation structure. They also stated that language in the House committee report accompanying the fiscal year 2015 DHS appropriations bill directed DHS to work with components and OMB, and the Committee to develop a common appropriation structure for the President's fiscal year 2017 budget request.8 S&T officials acknowledged that a common definition of R&D and a common appropriation structure that specifically includes R&D will make it possible to track all R&D within DHS. We believe that a common R&D definition that is consistently known and used by all DHS components will help ensure that components appropriately identify R&D activities, including contracts with industry, universities, and DOE's national laboratories. This will help DHS ensure that those types of R&D activities are accurately reported as R&D. In addition, we believe that a common appropriation structure will help ensure that all R&D activities occurring throughout the department are effectively tracked and reported and will help Congress have better oversight of DHS's R&D activities.

7DHS provided data on obligations to DOE national laboratories.
8H.R. Rep. No. 113-481, at 24 (2014) (accompanying H.R. 4903, 113th Cong.) H.R. 4903 has not been enacted.

2. In your written testimony, you noted the March 2014 conference to identify common problems centers have in accessing data from DHS. You said this was a step in the right direction, but can you speak on the key findings and recommendations from this conference?

Response:

As stated in our July 2014 testimony, the Office of University Programs (OUP) and the National Center for Border Security and Immigration—a DHS S&T Center of Excellence (COE) —co-hosted a workshop in March 2014 to identify common problems the centers have in accessing data from DHS, understand DHS constraints in sharing data, and develop best practices.9 According to the workshop summary provided by DHS officials, the workshop's key findings and recommendations include:

(1) Addressing how to build trust and align mission objectives between COE researchers and agency stakeholders by, among other things, potentially allowing or embedding university researchers to work or spend time with their agency stakeholders.

(2) Technical aspects of data sharing were discussed such as: how to identify data that can be shared; what can be done to mitigate data sensitivity concerns, such as removal or modification of identifying information; and how data quality issues can be addressed both before and after research takes place. In addition, according to DHS officials the workshop participants considered implementation and adoption of research findings by agencies.

(3) Standardization of processes to facilitate data sharing in the context of data sensitivity and privacy rules and regulations. The discussions included the identification of existing policies and how they might be better clarified and disseminated. Recommendations from the session included the creation of templates and standardized language, increased formalization of responsibilities and protocols, and increased focus on effective policy dissemination and training.

In July 2014, OUP officials provided us with additional information on the actions they are taking as a result of the workshop and its findings, such as

- Reaching out to the DHS components to discuss the outcomes of the workshop and to solicit how they can help facilitate data access for COE researchers. As part of the outreach effort OUP is seeking feedback, developing protocols, and establishing avenues to share best practices. For example, according to OUP, CBP's Plans and Policy Director is developing a "straw-man" protocol to follow to get access for COE researchers to CBP data.

9GAO, *Department of Homeland Security: Continued Actions Needed to Strengthen Oversight and Coordination of Research and Development*, GAO-14-813T (Washington, D.C.: July 31, 2014).

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY
SUBCOMMITTEE ON OVERSIGHT

"Technology Needed to Secure America's Border"

Mr. David C. Maurer, Director, Homeland Security and Justice, U.S. Government Accountability Office

Questions submitted by Rep. Scott Peters, Member, Subcommittee on Research and Technology

1. Regarding embassy perimeter security, a senior policy expert from RAND testified in 2012 about long-range communications technology, also called acoustic hailing devices, that can provide a non-lethal capability when used at very high volumes without causing any permanent harm. This communications and access denial technology is being used by the Army in Afghanistan, on ships by the Navy, and by police forces all over the world. What is the potential utility of such technology on the border? Has CBP reviewed or tested acoustic hailing devices in terms of their potential application on the border and if not, are you aware of a specific reason?

Response:

We have not reviewed CBP's non-lethal weapons (NLW) capabilities and CBP told us that there has not been a review or testing of NLWs recently. However, they told us there could be some use for such technology if a device works in the twisting and turning tunnel environment. Further, CBP indicated that testing of Long Range Acoustic Devices (LRADs) is planned for Fall 2014 in Nogales, Arizona.

In April 2009, we conducted work on the Department of Defense's (DOD) joint non-lethal weapons program, and some of our findings may be useful in future evaluations of CBP's NLW
Efforts.10 We found that, the joint NLW program conducted more than 50 research and development efforts and spent at least $386 million since 1997, but it had not developed any new weapons and the military services fielded 4 DOD items stemming from these efforts that only partially fill some capability gaps identified since 1998.11We found that three major factors contributed to the program's limited progress in fully addressing capability gaps:

- First, DOD did not prioritize department-wide non-lethal capability gaps until 2007.
- Second, DOD had not consistently incorporated logistics and supportability considerations early in the development process, which could result in missed opportunities to allocate resources more effectively.
- Third, DOD had exercised limited general oversight of the NLW program, which had resulted in gaps in key program guidance as well as limited measurement of progress and performance.

[10]GAO, *Defense Management: DOD Needs to Improve Program Management, Policy, and Testing to Enhance Ability to Field Operationally Useful Non-lethal Weapons*, GAO-09-344 (Washington D.C.: Apr. 21, 2009).
[11]The 4 programs that have completed the development process and been fielded by one or more of the military services were (1) 40 mm non-lethal crowd dispersal cartridge, (2) modular crowd control munitions, (3) portable vehicle arresting barrier, and (4) vehicle lightweight arresting device.

Appendix II

Additional Material for the Record

PREPARED STATEMENT OF FULL COMMITTEE
RANKING MEMBER EDDIE BERNICE JOHNSON

OPENING STATEMENT

Ranking Member Eddie Bernice Johnson (D-TX)
Committee on Science, Space, and Technology

Joint Subcommittee Hearing
Subcommittees on Research & Technology and Oversight
"Technology Needed to Secure America's Border"
July 31, 2014

Thank you Mr. Chairman. The issue before us today is an important area within this Committee's jurisdiction. This can be a constructive hearing if Members focus on the science and technology concerns at the Department of Homeland Security and not let it turn into a forum for debating the ongoing events at the Southwest border or other issues related to our immigration system. There are other venues for those debates, and those broad issues cannot be solved with new technologies. However, there are many threats that can be addressed with technological innovations.

As a Texan, I fully understand the complex challenge of securing our nation's borders. Detecting and preventing the illegal entry of dangerous individuals and substances is the highest priority of the U.S. Customs and Border Protection agents. Protecting America's border requires innovations that keep us ahead of those who wish to do us harm. Innovation begins with investment in R&D. It is the responsibility of this Committee to provide oversight of the Department's research activities to ensure the most effective technologies and innovative solutions are provided to the agents and other operators on the front lines.

DHS has experienced many growing pains during its first ten years. Technology failures are an accepted part of the research process and are indicative of R&D that is on the cutting edge. However, government failures due to inadequate testing and evaluation or poor coordination within the agency cannot be an accepted pattern at the agency. I look forward to hearing about potential improvements that could be made to ensure DHS R&D investments are well-managed.

While it is unfortunate that we are not hearing from DHS today, I look forward to GAO's recommendations on what DHS can do to improve the process of transitioning useful technologies to the field while limiting waste and duplication. I understand DHS's Under Secretary for Science and Technology will be appearing before the Committee soon and the recommendations from these experts here today should provide useful input to that discussion.

Such recommendations will also inform our thinking as we begin discussions of a reauthorization of the DHS Science & Technology Directorate with our colleagues on the Homeland Security Committee.

In closing, I want to welcome our witnesses to this hearing and I look forward to your testimony. With that, I yield back the balance of my time.

ADDITIONAL SUPPORTING INFORMATION REQUESTED BY
FULL COMMITTEE CHAIRMAN LAMAR S. SMITH

PETRO DATA COMM, LLC
www.petrodatacomm.com

July 30, 2014

Congressman Lamar Smith
US House of Representatives
21st District of Texas
2409 Rayburn House Office Building
Washington, DC 20515

Honorable Congressman Smith,

At the request of your Legislative Assistant, Chris Shank, Petro Data Comm, LLC humbly submits the following information for your review and consideration and presentation to your Science & Technology Committee, as a solution to the extremely limited and in many areas, non-existent, bandwidth and broadband services, which highly curtail the US Office of Homeland Security and the US Border Patrol's ability to properly secure our US Borders.

Petro Data Comm, LLC, hereinafter referred to as PDC, was originally formed to provide state of the art high speed, broadband communications services to the Oil and Gas Industry as a permanent solution for the delivery of the extremely voluminous files of data, which are now being produced by the new emerging technology of DAS/DTS Fiber Optic Sensing of hydrocarbon reservoirs.

DAS/DTS (Distributive Acoustic Sensing / Distributive Temperature Sensing), of hydrocarbon reservoirs, is the new technology of permanently installing a Fiber Optic Cable adjacent to, but just outside of the casing pipe or clamped to the production tubing, from the surface of a well to the bottom of the wellbore, to act as a sensor, to monitor the sounds which are produced in the wellbore for the *entire life of the well*. The sounds produced represent a particular event, which has occurred in the reservoir and by the use of algorithms, within the proprietary software and hardware installed on the surface of the well, geophysicists and geologists are able to determine what event has occurred and what needs to be done to correct a problem.

Unfortunately for the oil and gas industry the limited bandwidth, which has been traditionally available from Internet services providers in remote areas, is not capable of delivering these voluminous files of data to the analytical departments of corporate headquarters, in "Real Time". Therefore, an engineer or some designated company representative has to physically go to the well site and retrieve the hard drive from the proprietary server on the surface of the well and return it to the analytical department of their corporate headquarters to be analyzed.

In addition to the use of fiber optic cable in the wellbore to monitor reservoir activity, when a fiber optic cable is buried in the ground, within three feet of a pipeline the fiber optic cable is able to monitor leak detection and any intrusion of the pipeline, such as "Hot Tapping" or vandalism.

In fact, the fiber optic cable is so sensitive that when installed above ground it is capable of delivering precise voice communications to military, law enforcement, security personnel, cloud storage facilities or any other designated recipient in "Real Time".

10730 Potranco Road, Suite 122-156, San Antonio, TX 78251

As PDC has moved forward, with our research, in our quest to provide a state of the art communications system for the delivery of these voluminous files of data, from hydrocarbon reservoirs, pipelines and above ground perimeter security, we have discovered an unsatisfied need for high resolution video cameras, capable of delivering an unlimited number of streams of smooth flowing, uninterrupted live video to security personnel, corporate executives, cloud storage facilities, local and federal law enforcement agencies in "Real Time" as well.

To meet that unsatisfied need, PDC has teamed up with three well established technology partners to form, "Petro Surveill", a new division of PDC, which is now offering a self contained video surveillance system, which consists of a high resolution vehicle recognition camera coupled with PDC's state of the art, proprietary, high speed, broadband communications system. This new system has been designed to meet the need for video surveillance cameras in numerous roles, including, but not limited to, oil and gas fields, hubs and terminals, water plants, pipelines, nuclear plants, refineries, chemical plants, defense contractor facilities, maritime ports, corporate headquarters and any and all other high profile targets of terrorism, world wide, and our US borders.

To sum up all of the aforementioned technology, PDC has focused on a state of the art communications system, which is capable of delivering extremely voluminous files of data, wherever and whenever directed by a customer, in "Real Time", regardless of whether that data is produced from DAS Fiber Optic Sensing of a wellbore, a pipeline, above ground perimeter surveillance or PDC's High Resolution Video Cameras!

Petro Data Comm, LLC welcomes the opportunity to be considered as a US government contractor to provide bandwidth services and video surveillance systems in the remote areas of our southern US Borders and any and all other areas which may currently be or may become targets of terrorism or of concern to our US Office of Homeland Security.

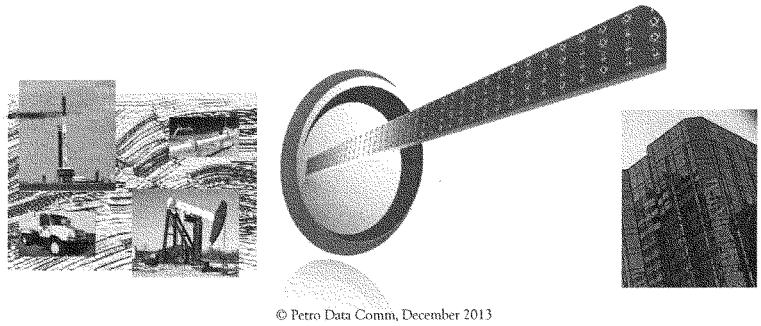
Additional information will be provided upon request.

Respectfully,
Robert W. Carey, Jr.
Executive VP, Marketing
830-377-3600

PETRO DATA COMM

Communications Specialists for the Digital Oil & Gas Field

Contact: Mr. RW (Bob) Carey, Jr. 830.377.3600



© Petro Data Comm, December 2013

Field Production & Exploration

Preparing for the digital oil & gas field is best begun after permit approval or even before. Oil field technologies are rapidly increasing in complexity – as is the business and regulatory environment. Is the communication infrastructure in your upstream oil and gas field in place? We can support you to ensure your field communications network can provide the real time and data intensive performance demanded by advanced down hole and reservoir management technologies.

Operations & Contractor

Field staff and contractor communications needs begin when clearing and mobilization begins and continues throughout all phases of the drilling, completion, production, and later workover cycle; but does it end there? Let us plan, implement and maintain your operation's communication facilities in the field. We provide facilities management and maintenance for a sustained long term communications network. To include SCADA but beyond, to the emerging digital technologies. We can work with your IT and field automation groups; or as you IT and field automation specialist to provide turnkey facilities infrastructure and management.

Facilities Integrity & Security

From gate security to perimeter security, from video surveillance to pipeline integrity & security, use our cloud services and our communications and security systems engineering, implementation, and maintenance skills to protect your assets 24 x 7 x 365.

Workover and Completion

Down hole acoustic and thermal data can be acquired, processed, and monitored during **workover and completion** activities, down hole and in real time. With new and emerging sensor technologies, and if the operator prepares ahead for it, permanent sensors and communications facilities can be put into place to facilitate workover and completion activities without requiring invasive sensor systems. Let us prepare your field communications facilities so that you can achieve the operational efficiencies most only dream of today.

Long Term Reservoir Management & Regulatory Monitoring

Let us plan, design, and construct your field communications facilities so that you can use advanced & emerging technologies for increasing recoverable oil and gas reserves; and use the same facilities to support your operational compliance with regulatory requirements.

10730 Potranco Road
Suite 122-156

www.petrodatacomm.com

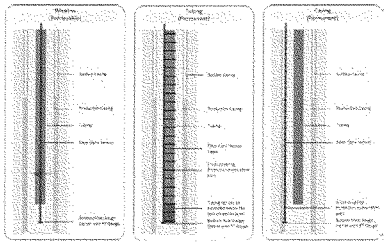
San Antonio, TX 78251

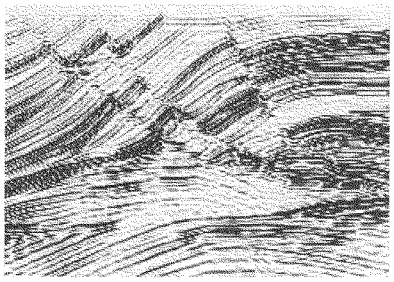
© Petro Data Comm, December 2013

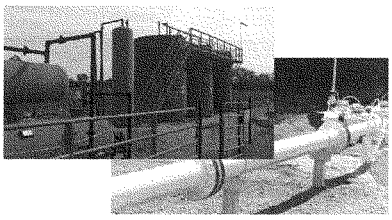
PETRO DATA COMM

Communications Specialists for the Digital Oil & Gas Field
Contact: Mr. RW (Bob) Carey, Jr. 830.377.3600

Why is a Communications Specialists needed to bring long term communications network infrastructure to the Digital Oil & Gas Field? Imagine you're an oil or gas company and you learn that you can acquire new, but field proven, advanced technology that enables a (very modest) 1% improvement in hydrocarbon recovery. As an example, a large field in Saudi Arabia is worth $10 billion today, a 1% improvement in reserves recovery represents an additional $100 million revenue – in only one field. Now imagine not being able to utilize that new advanced technology because there is not sufficient communications infrastructure serving your installations. Petro Data Comm is created to provide the communications network infrastructure in field locations as needed to enable the advanced technologies being introduced to the 'digital oil and gas field'.







Digtributd Accoustical (DAS) & Temperature (DAT) Sensing

Oil and Gas Well/Field – *real-time observation*

- Efficiency and efficacy of well completion
- Well bore characterization
- Fluid flow logging – continuous
- Seismic Acquisition – Vertical Seismic Profiling and micro-seismic detection, real-time and during production
- Long term reservoir management – seismic acquisition during well production
- Answer the question, with hard data, of 'when' do I stop drilling injection wells?
- CO_2 Sequestration monitoring -Regulatory

OptaSense: **"OptaSense proven technology is fundamentally changing the approach to significant areas of Oil Field Services management"**

Halliburton: **"The next stage of well monitoring Fiber optic sensing technology represents the future of well monitoring. Advanced techniques in fiber optic technologies are providing a complete, real-time view of downhole conditions without any wellbore intervention."**

Asset Integrity & Security

- Pipeline leak detection
- Pipeline PIG tacking
- Detection of third party intrusion for full length of pipeline
- Passive monitoring for site security

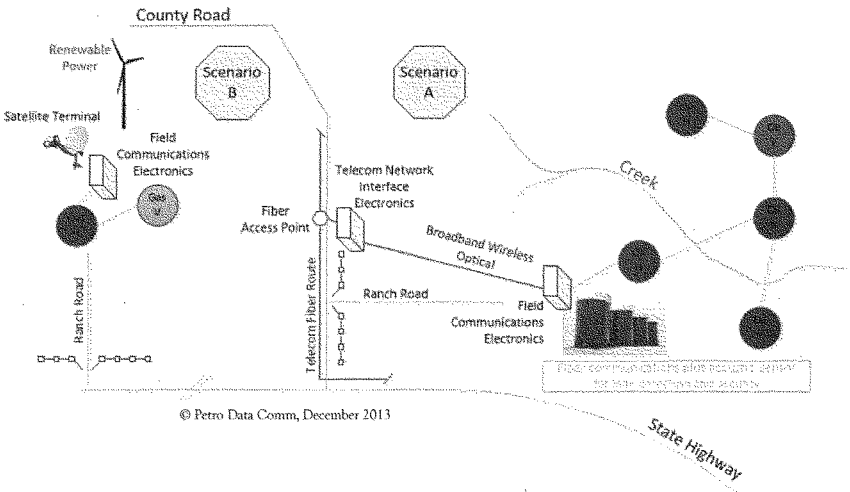
10730 Potranco Road
Suite 122-156

www.petrodatacomm.com

San Antonio, TX 78251
© Petro Data Comm, December 2013

PETRO DATA COMM
Communications Specialists for the Digital Oil & Gas Field
Contact: Mr. RW (Bob) Carey, Jr. 830.377.3600

EXAMPLE FIELD INSTALLATIONS



© Petro Data Comm, December 2013

(A) Scenario A: A common implementation utilizing mesh wireless routers or private fiber optic cables to interconnect numerous well sites for interconnection with a broadband terrestrial fiber communications network.

(B) Scenario B: A remote and isolated well site may utilize ***broadband*** satellite communications for connection to the Internet and Office WAN

(C) Combination Scenario: An installation may route data through multiple communications technologies at the field site to achieve the lowest cost broadband service for transport of total data requirements.

NOTE:
The private fiber optic communications cable can, in addition to providing a broadband communications link, be utilized for monitoring of pipeline security and leak detection. Total pipeline length can be monitored in one or more segments of up to 100 Km lengths and each segment may be up to 100 Km in length.

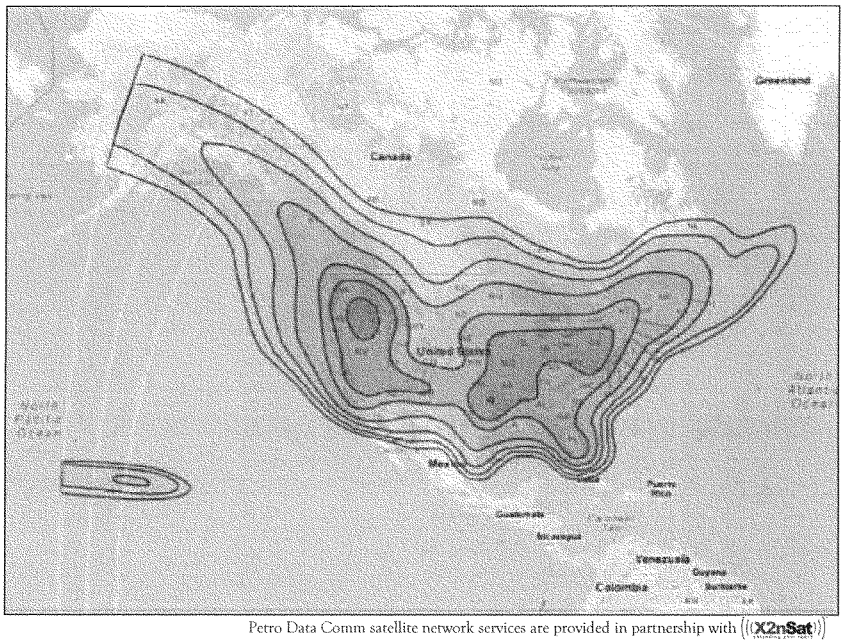
© Petro Data Comm, December 2013

PETRO DATA COMM
Communications Specialists for the Digital Oil & Gas Field
Contact: Mr. RW (Bob) Carey, Jr. 830.377.3600

Satellite Coverage Maps

Petro Data Comm utilizes multiple spacecraft to facilitate total coverage of the North American continent, including outlying areas as noted in the diagrams below. Coverage can be evaluated for locations outside of North America on a per-site basis.

Ku-Band Coverage on SES-2 Satellite



Petro Data Comm satellite network services are provided in partnership with ((X2nSat))

10730 Potranco Road
Suite 122-156

www.petrodatacomm.com

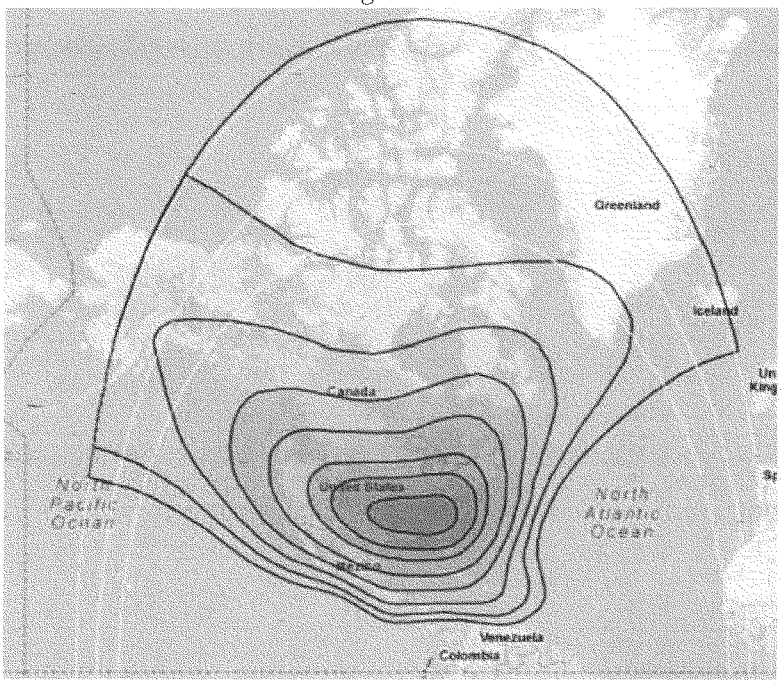
San Antonio, TX 78251
© Petro Data Comm, December 2013

PETRO DATA COMM
Communications Specialists for the Digital Oil & Gas Field
Contact: Mr. RW (Bob) Carey, Jr. 830.377.3600

Satellite Coverage Maps

Petro Data Comm utilizes multiple spacecraft to facilitate total coverage of the North American continent, including outlying areas as noted in the diagrams below. Coverage can be evaluated for locations outside of North America on a per-site basis.

C-Band Coverage on SES-2 Satellite



Petro Data Comm satellite network services are provided in partnership with X2nSat

10730 Potranco Road
Suite 122-156

www.petrodatacomm.com

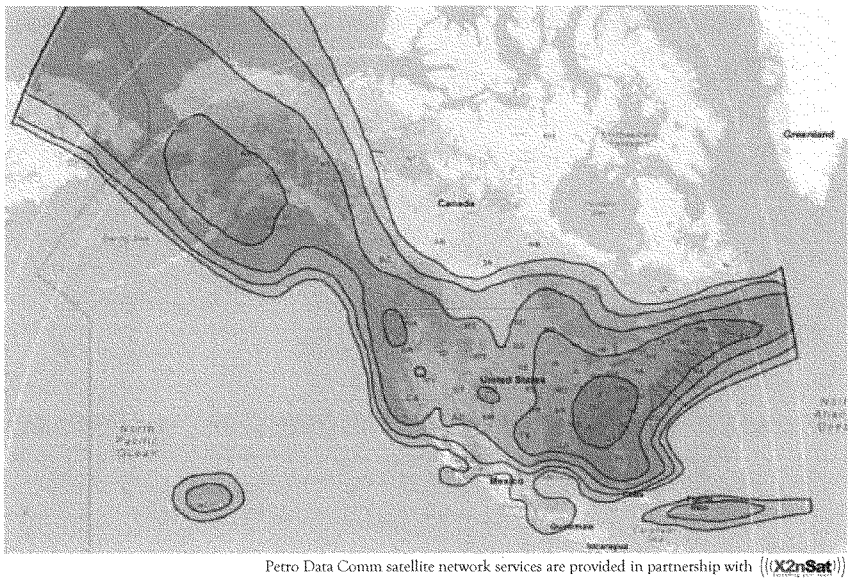
San Antonio, TX 78251
© Petro Data Comm, December 2013

PETRO DATA COMM
Communications Specialists for the Digital Oil & Gas Field
Contact: Mr. RW (Bob) Carey, Jr. 830.377.3600

Satellite Coverage Maps

Petro Data Comm utilizes multiple spacecraft to facilitate total coverage of the North American continent, including outlying areas as noted in the diagrams below. Coverage can be evaluated for locations outside of North America on a per-site basis.

Ku-Band Coverage on Horizons 1 Satellite



Petro Data Comm satellite network services are provided in partnership with X2nSat

10730 Potranco Road
Suite 122-156

www.petrodatacomm.com

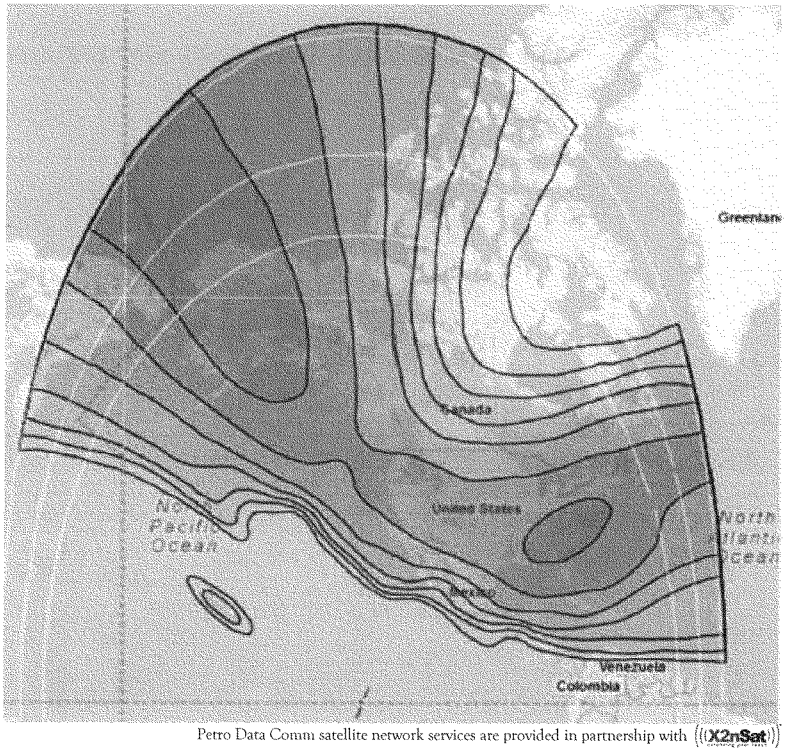
San Antonio, TX 78251
© Petro Data Comm, December 2013

PETRO DATA COMM
Communications Specialists for the Digital Oil & Gas Field
Contact: Mr. RW (Bob) Carey, Jr. 830.377.3600

Satellite Coverage Maps

Petro Data Comm utilizes multiple spacecraft to facilitate total coverage of the North American continent, including outlying areas as noted in the diagrams below. Coverage can be evaluated for locations outside of North America on a per-site basis.

C-Band Coverage on Horizons 1 Satellite



Petro Data Comm satellite network services are provided in partnership with ((X2nSat))

© Petro Data Comm, December 2013

PETRO DATA COMM
Communications Specialists for the Digital Oil & Gas Field
Contact: Mr. RW (Bob) Carey, Jr. 830.377.3600

Broadband Connectivity via Satellite

High Bandwidth – Large Data Volume

Petro Data Comm's Broadband connectivity allows operators a high-bandwidth – large volume, ***point-to-point*** and ***point-to-Internet*** connection via satellite - providing maximum efficiency, clear channel capacity. Dedicated Broadband is unshared, meaning you have a guaranteed connection providing the bandwidth you require for your applications and logistics.

Guaranteed Connectivity & Speed

Often compared to terrestrial leased-line connections, Dedicated Broadband is ideal for any organization requiring consistent bandwidth that cannot chance the potential delays or reductions in service inherent in a shared connection. Rather than sharing the bandwidth with other users, our Dedicated Broadband puts the power in your hands, allowing you to allocate the precise amount of bandwidth you need for your applications, from 64 Kbps all the way up to 155 Mbps, outbound or inbound. Use this bandwidth for a multitude of applications – even - imagine your own virtual satellite hub with on-demand bandwidth allocation via our easy-to-use interface.

Network Diversity

With a diversity of spacecraft linked to teleports and data-centers spread throughout North America and Globally, Petro Data Comm's satellite network has C and Ku-Band capability with multiple redundancies.

Pricing

Customizable pricing with pay-per-byte or fixed monthly charge with monitored Fair Access Policy.

Customizable

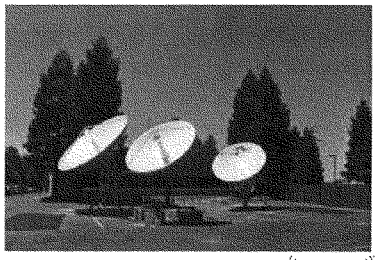
Set the bandwidth you need in the network configuration that best suits your needs. For maximum user flexibility, Petro Data Comm's Dedicated Broadband can be configured as Point-to-Point, Star or Mesh network topologies.

Shared Broadband Service

Petro Data Comm's Shared Broadband Service plans are designed for clients looking for general internet broadband connectivity. These plans give users high quality Broadband Internet experience and allow competitive price points in relation to other local wireless options such as 3G/4G services from AT&T and Verizon.

Data Security

All Internet transported data is encrypted and transported to the customer's data center via a Virtual Private Network tunnel. Dedicated Broadband is one of the most secure forms of data transfer available, it is considered a closed network due to its point-to-point path. This means your data is entirely private and does not travel over any form of public network as it would through typical communications infrastructure.



Petro Data Comm satellite network services are provided in partnership with X2nSat

10730 Potranco Road
Suite 122-156

www.petrodatacomm.com

San Antonio, TX 78251
© Petro Data Comm, December 2013

PETRO DATA COMM
Communications Specialists for the Digital Oil & Gas Field
Contact: Mr. RW (Bob) Carey, Jr. 830.377.3600

Broadband Connectivity via Satellite

Customer Service is Our Buiness

When you need support, we are not satisfied with forcing you to conform to a rigid structure of low-level troubleshooting and slow escalation models. Petro Data Comm was built upon a platform of flexibility and customization for our clients and we prove this with our levels of support.

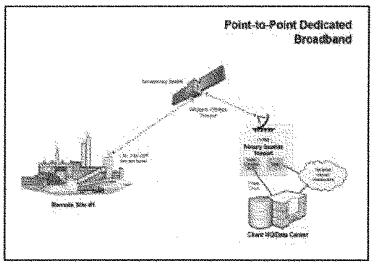
- 24x7x365 observation of all client connections. Allows for error preemption and mitigation.
- Technicians have a direct view of our primary data center and satellite array.
- 95% of support calls never wait in a queue, 95% of calls satisfied in real-time before call ends, 95% of calls are resolved after speaking with the 1st technician.
- Petro Data Comm's proprietary support ticketing system records all data to efficiently troubleshoot future issues.
- Clients can create their own support tickets through our private web portal, including requests for engineering consultations and higher-tier technicians.
- California-based main teleport maintains extremely high availability.
- Redundant teleport in Atlanta, GA
- Consistent latency with 99.9% annual service reliability 24x7x365

Network Support

Support and network monitoring through our Network Operations Center. Petro Data Comm operates a fully staffed 24x7x365 Network Operations Center located on-site at our primary teleport and data center in California.

Enterprise –Specific Provider

Petro Data Comm is a commercial/enterprise specific solution provider, we do not service residential or general consumer markets. With private, secure and unsaturated networks and support, Petro Data Comm is an efficient and highly responsive communications partner.



Customized Network Solution

Petro Data Comm's engineers tailor your solution to your current infrastructure, rather than forcing you to conform to a rigid solution set. This will allow us to make our solution completely seamless to your network and IP addressing environments as they are today. And – guaranteed QoS levels.

Petro Data Comm satellite network services are provided in partnership with X2nSat

10730 Potranco Road
Suite 122-156

www.petrodatacomm.com

San Antonio, TX 78251
© Petro Data Comm, December 2013